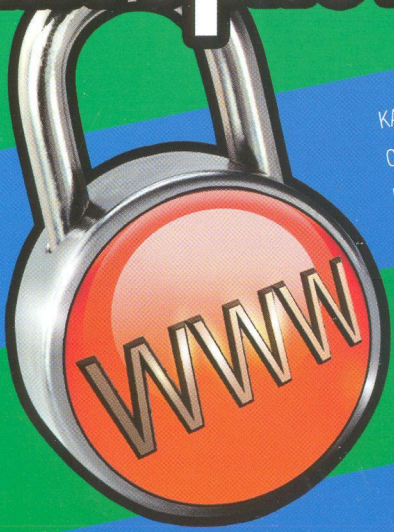
VISIT…

Компьютер это просто

Виталий Леонтьев

Безопасность в сети Интернет



КАК РАСПОЗНАТЬ СЕТЕВОЕ МОШЕННИЧЕСТВО

КАК СОХРАНИТЬ СВОИ ПАРОЛИ В БЕЗОПАСНОСТИ

ОТКУДА ПОЯВИЛИСЬ ВИРУСЫ И КАКИЕ ОНИ БЫВАЮТ

КАК ЗАЩИТИТЬСЯ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

КАК ОБЕСПЕЧИТЬ СЕБЕ КОНФИДЕНЦИАЛЬНОСТЬ В СЕТИ

Компьютер это просто

Виталий Леонтьев

Безопасность в сети Интернет

МОСКВА
ОЛМА Медиа Групп
2008

УДК 004
ББК 32.973
Л47

Леонтьев В.П.

Л47 Безопасность в сети Интернет. — М.: ОЛМА Медиа Групп, 2008. — 256 с.: ил. — (Компьютер — это просто!)

ISBN 978-5-373-01819-7

Вместе с Интернетом в нашу жизнь вошли такие явления, как компьютерные вирусы, «трояны», спам и другие не слишком приятные вещи. Новая книга Виталия Леонтьева поможет как опытному, так и начинающему пользователю максимально обезопасить свой компьютер от атак из Сети. Кроме того, в справочнике есть обзор видов сетевых афер, вирусов, рекламных модулей. И, конечно, перечень пакетов программ, защищающих компьютер от незваных гостей. Книга написана живым и простым языком.

УДК 004
ББК 32.973

ISBN 978-5-373-01819-7

© ЗАО «ОЛМА Медиа Групп», издание, 2008

Предисловие

До чего же парадоксальна человеческая натура! Ведь каждый божий день мы слышим о все новых и новых кознях хакеров, меланхолично фиксируем появление новых вирусов, сокрушаемся о нестабильности и уязвимости существующих информационных систем... И в то же время не делаем ничего, чтобы хоть как-то обезопасить свой собственный компьютер! Более того, — даже не знаем, какие именно опасности могут нам встретиться на информационной магистрали.

А их не так уж мало. При всей своей внешней дружелюбности дорога Интернета отнюдь не вымощена желтым кирпичом, на ней и ухабы не редкость, да и замаскированные ямы с кольями на дне попадаются. Другое дело, что для многих «хищников» наш брат пользователь — слишком мелкая дичь. И потому на ваш компьютер, подключенный к Сети в сеансовом режиме, через слабенький модемный канал, вряд ли станут покушаться серьезные хакеры. Из тех, которых хлебом не корми, а дай «завалить» серьезный сервер

какого-нибудь Пентагона. И содержимое вашего винчестера не улетит за считаные секунды в бездну Интернета (этот потрясающий пассаж автор вычитал в опусе одного из мэтров отечественной фантастики), «вытянутое» тем же загадочным «взломщиком».

Все это — опять-таки, для нас, пользователей, — не страшнее бумажного тигра. Однако и настоящих тигров не так уж мало, и встреча с ними вам в большинстве случаев никаких приятных эмоций не доставит.

Так что о защите подумать не помешает. Но прежде все-таки надо узнать, от чего именно мы будем защищаться. Так что пересчитаем и поименуем имеющуюся полосатую нечисть.

УГОЛОК ОСТАПА БЕНДЕРА: СЕТЕВЫЕ АФЕРЫ

В Интернете, как известно, есть все — даже то, чего пока что не существует в природе.

И было бы просто удивительно, если бы там не появились мошенники и «кидалы» всевозможных сортов — даже те, что в природе давно уже вымерли.

От банальных рулеточников и наперсточников, зазывающих нас яркими вывесками Интернет-казино и всевозможных пирамид, до более изощренных наследников Остапа Бендера, который, получи он доступ к Интернету, моментально изобрел бы еще пару тысяч способов сравнительно честного отъема денег у населения. А потому грех не посвятить этому, сколь увлекательному, столь и опасному явлению, хотя бы пару страниц в нашей книге.

Вообще-то составить список ВСЕХ возможных афер и надувательств в Сети невозможно — хотя еще в 2001 году Федеральная Торговая Комиссия США попыталась это сделать.

Составленный краткий список основных видов мошенничеств с использованием Сети выглядит так:

- **Мошенничество на аукционе.** Продажа некачественного товара или отказ предоставить товар после завершения торгов. Этот вид мошенничества лидирует и в России: с махинациями на аукционах и барахолках связано более 40 процентов всех сетевых афер.

- **Мошенничество Интернет-провайдеров**. Кража денег со счета клиента, «накручивание» счетчика трафика и т. д. В российских условиях встречается довольно редко.

- **Дизайн и позиционирование веб-сайта.** Внешний вид посещенного вами сайта может дать обманчивое представление о его содержании.

- Информационное мошенничество и услуги для взрослых: **взлом кредитных карт**. К этому виду преступлений относится создание «липовых» порно-сайтов и Интернет-магазинов, а также кража номеров кредитных карточек из баз данных вполне благонадежных сайтов.

Многоуровневый маркетинг, мошенничество посредством построения экономических пирамид. Системы типа «Привлеките 10 друзей к участию в нашей рекламной компании — и ваш заработок обеспечен!». Как правило, материальный ущерб от таких игр не слишком высок, в отличие от потери времени и сил.

Деловые предложения. С помощью электронной почты или веб-сайта нетрудно выдать себя или свою фирму за крупную и обеспеченную компанию. Учтите — по-настоящему серьезные фирмы никогда не рассылают своих предложений кому попало. Ни по электронной, ни по обычной почте.

Инвестиционные схемы типа «Станьте богатым прямо сейчас». Самый опасный вид мошенничества. Именно к такому типу относится известная «нигерийская афера», а также многочисленные аферы с «виртуальными инвестиционными фондами».

Мошенничество с туристическими путевками. Продажа поддельных туров или тайм-шеров.

Телефонное мошенничество (платные звонки).

Мошенничество в сфере охраны здоровья.

Сегодня к этому списку мы смело могли бы добавить еще несколько, а то и несколько десятков пунктов. Однако читать такие списки скучно, тем более, что в России многие схемы попросту не работают — зато появляются новые, невиданные доселе формы надувательства.

Поэтому совершим пробежку по самым распространенным и опасным аферам, с которыми можете столкнуться именно вы. Но сначала — несколько рекомендаций, как хотя бы отчасти застраховать себя от козней сетевых жуликов. Возможно, каждый из этих признаков по отдельности и не свидетельствует о скрытой ловушке, но если таких признаков несколько...

⏭ Бойтесь «халявы»! Бесплатный сыр и в сети бывает только в мышеловке: если вам предлагают нужный товар по цене в несколько раз дешевле обычной, задумайтесь, кто из вас двоих идиот. Продавец — или вы, уже гостеприимно открывший ему свой кошелек?

⏭ НИКОГДА — повторяю, НИКОГДА не платите за товар вперед, если вам предлагает его неизвестный магазин типа «Озона», а частное лицо или сомнительная «барахолка».

⏭ Остерегайтесь виртуальных магазинов с доменами третьего уровня, расположенных на

серверах «бесплатного хостинга» (da.ru, narod.ru, freemail.com и т. д.).

⏭ НИКОГДА не работайте с продавцами или магазинами, на сайтах которых вы не найдете контактного адреса и телефона! Контакты с продавцом по e-mail не являются надежной гарантией безопасности сделки.

⏭ Остерегайтесь российских магазинов или сайтов, расчет с которыми возможен лишь с помощью «электронных платежей» (WebMoney, Яndex.Деньги). Помните — в отличие от платежей через «виртуальный кошелек», платеж по кредитной карте можно блокировать, обратившись в службу безопасности банка.

⏭ Старайтесь пользоваться услугами проверенных, надежных сайтов, входящих в рейтинги поисковых служб и в крупные каталоги (Rambler, Mail.Ru). Перед сделкой попытайтесь найти отзывы о сайте других покупателей через поисковые системы или, в случае с западными сайтами, через сервер Epinion (http://www.epinions.com).

⏭ На западных сайтах ВСЕГДА читайте раздел вопросов и ответов (FAQ) или Terms and Conditions.

⏭ Если для доступа к большинству своих разделов сайт требует открытия платного

аккаунта, не гарантируя в случае его отмены возврат денег — это откровенное мошенничество.

⏭ Обращайте внимание на присутствие на российских сайтах РАБОТАЮЩЕГО форума или гостевой книги.

⏭ Никогда не высылайте номер своей кредитной карты почтой — оформляйте сделку только через систему безопасных транзакций (ее используют все серьезные сайты).

⏭ Заведите специальную пластиковую карту для сетевых платежей, при этом сумма на ней в любой момент времени не должна быть больше, чем необходимо вам для одной покупки. Хлопотно — зато безопасно.

«Нигерийские письма»

«Нигерийская афера» или «мошенничество 419» (имя этот трюк получил по номеру соответствующей статьи в нигерийском уголовном кодексе) существовала задолго до появления Сети — по крайней мере, еще в начале 80-х годов тысячи американцев находили в своих почтовых ящиках письма вот такого типа:

«К вам обращается MR. GEORGE KABILA, брат последнего президента Республики Конго Лорента Кабилы. Информацию о Вас я нашел в... Будьте информирован, что мой осведомитель не знает о природе бизнеса, у которого я спрашиваю вашу помощь. У меня есть выгодное предложение для вас. После убийства моего брата, бывшего президента Лорента Кабилы, и перехода власти к его сыну Джозефу, мы обнаружили, что некоторая сумма денег (25,500,000.00 американских долларов) теперь помещена на банковский счет в Швейцарии для нашего личного использования.

К сожалению, я не имею средств для перевода денег в другой банк и разморозки счета... Именно поэтому я обращаюсь к вам. Если Вы согласны компенсировать мои расходы по переводу счета, вы можете получить в качестве вознаграждения до 30 % имеющейся на счете суммы».

Названия стран, как и почивших правителей, все время меняются (сегодня письма приходят уже от наследников Саддама Хусейна и Бен Ладена). Да и дислокация мошенников отнюдь не ограничивается территорией Нигерии (где почтовыми аферами занимаются целые семейные кланы). Однако суть остается прежней.

Стоит ли говорить, что, получив в свое распоряжение номер банковского счета или кредитной карточки, мошенники не останавливались, пока не опустошали этот счет до дна. Хотя гораздо ча-

ще сами жертвы послушно делали перевод за переводом, ожидая обещанных сокровищ.

Как ни странно, даже такая насквозь прошитая белыми нитками сказочка находит своих благодарных слушателей. Только в 2002 году на эту нехитрую приманку, по подсчетам Национального центра по расследованию экономических преступлений США, клюнуло более 2600 человек, а доход дельцов «нигерийского бизнеса» составил более 5 миллиардов долларов! Шумный резонанс получила прошлогодняя драма в Праге, когда разоренный «нигерийцами» 72-летний пенсионер застрелил консула Нигерии в его собственном офисе.

В России пострадавших от действий «нигерийцев» пока что не зафиксировано — однако причиной этого можно считать лишь крохотное количество обладателей персональных счетов в западных банках, а отнюдь не излишнюю грамотность местных интернетчиков.

«Фишинг»

Представьте себе, что вы пользуетесь нелицензионной (а проще говоря — пиратской) копией Windows... Нет, я знаю, что такой кошмар

представить просто невозможно — но вы все же попробуйте. Ну вот, а теперь вообразите, что однажды в ваш почтовый ящик падает письмо от рекламного отдела Microsoft, где вам предлагают зарегистрировать вашу копию и стать владельцем абсолютно легальной программы всего... за один доллар! Только сделать это можно в течение часа — таковы, мол, условия рекламной акции.

Вы щелкаете по приложенной в письме ссылке — и действительно, попадаете на сервер Microsoft, где вам предлагается немедленно оплатить покупку. Обалдев от счастья, вы лихорадочно вбиваете в специальную форму данные вашей кредитки, нажимаете OK — и уже готовитесь бежать на почту за оправленной вам коробкой. Увы, и через неделю обещанный сертификат вам не приходит, зато с вашего карточного счета улетучивается круглая сумма.

Как же так? Неужели Microsoft, отчаявшись заработать на продаже Windows Vista, начала банально чистить кошельки?

Конечно же, нет — столь грубыми методами компания Билла Гейтса не пользуется. Вы всего лишь попались на удочку мастеров «фишинга», сумевших закамуфлировать под сервер Microsoft совершенно «левый» сайт, цель которого — вытащить из вас вожделенный номер кредитки. Это, впрочем, мог быть и сайт Amazon.Com,

российского «Озона» или любого другого магазина, принимающего к оплате кредитные карточки.

Секрет мошенников прост: подобрать внушающий доверие адрес (например, www.amason.com вместо www.amazon.com) и полностью скопировать дизайн сайта-оригинала. Остальное — дело техники.

Российские пользователи с этой забавой до недавних пор не сталкивались — в Интернет-магазинах мы совершаем покупки нечасто, да и кредитки водятся не у каждого. Однако на Западе эпидемия фишинга приняла такой размах, что специалисты по безопасности всерьез озаботились этой проблемой. Достаточно сказать, что еще в конце 2005 года корпорация Symantec зарегистрировала более 30 миллионов (!) фишинг-атак, многие из которых увенчались-таки успехом...

Именно по этой причине во всех браузерах нового поколения — Internet Explorer 7, Firefox 2 и Opera — появились специальные фишинг-фильтры, способные с лету распознать подделку. Во всяком случае, если червячком на крючке «фишеров» становятся брэнды крупных компаний. Так что не забудьте включить фишинг-фильтр в вашем браузере — и чувствуйте себя относительно спокойно.

«Порно-сайт» и «магазин конфиската»

Этот вид махинации — один из самых распространенных в Сети, благо покупателей на сетевую «клубничку» всегда находится немало. И, несмотря на свою долгую и бесславную историю, эта схема великолепно работает и поныне.

Для создания такого сайта нужно немногое — пара десятков эротических фотографий, надерганных с бесплатных сайтов, и простенькая форма покупки «полного доступа». Чем завлекательнее и необычнее выглядит витрина такого сайта, тем больше шансов, что нерадивый охотник до сладкого попадет в расставленную ловушку. И действительно — один-два человека из тысячи, пересмотрев фотографии-«приманки», решат прикупить доступ и ко всему архиву...

После заполнения регистрационной формы (в которой наверняка найдется место для поля ***Номер кредитной карты***) покупатель перебрасывается на другой, бесплатный сайт, а то и вовсе в никуда. А ключик к его банковскому счету (в виде номера кредитной карты) оказывается в лапах предприимчивых мошенников...

Точно такой же фокус мошенники проворачивают, используя в качестве приманки витрину «виртуального магазина» с необычайно низкими ценами. В 2004–2006 годах в Рунете прокатился вал рекламных писем о «распродаже конфиската» по ценам в несколько раз дешевле обычных. Вариант этого мошенничества — предложение воспользоваться для покупки товаров услугами таинственных «хакеров», сумевших украсть номера кредиток у богатых Буратино из-за океана. Общие черты все этих афер — стопроцентная анонимность продавцов и требование предоплаты с помощью анонимных платежных систем (Яндекс.Деньги, WebMoney и т. д.).

«Free GSM»

Появление этой гениальной схемы мошенничества в 2001–2002 годах связано с двумя факторами — массовым распространением мобильных телефонов... И невероятной жадностью сотовых компаний, вздувших свои тарифы до совершенно неприличных величин. Иначе как объяснить то, что жертвами аферы оказались не только традиционно нищие студенты, но и вполне приличные представители среднего класса?

Сэкономить на сотовой связи хотелось всем — и немудрено, что вскоре в Интернете появился первый сайт с текстом следующего содержания:

Однажды, когда я прислушивался к очередному рекламному ролику про снижение тарифов одной сотовой компании (абонентом которой тогда являлся), я вдруг понял, какой же это идиотизм: с жадностью вслушиваться в текст рекламы, в надежде на скидку в пару центов, искать внизу маленькую надпись «без учета НДС», разговаривая по мобильному телефону, думать не о самом разговоре, а о том, на какую сумму я уже наговорил. Притом, что в «дальнем зарубежье» принято платить не более 20 долларов за безлимитный тариф в месяц. И это на фоне того, что наши операторы получают по 400–600 % прибыли (такого не было со времен «челночества"). В общем, я решил применить данные мне институтом ХИРЭ (Харьковский институт радиоэлектроники) знания.

Начал с изучения протокола GSM и просмотра информации, накопленной на подобную тему в Интернете. Результат был малоутешительный: сам стандарт GSM настолько защищен, что взломать его практически невозможно или, скажем так, настолько дорого, что отпадает сам смысл взлома. Повозившись еще немного, скорее для самооправдания, чем для дела, я все это забросил.

И вот в такой критический момент один случай натолкнул меня на мысль попробовать действовать

немного с другой стороны, а именно со стороны программного обеспечения сервера. Выяснилась одна интересная деталь. Если вы знакомы со стандартом GSM, то наверняка знаете, что пароли ASN постоянно меняются, сохраняясь на сервере и SIM-карте вашего телефона. Теоретически, создать клон такого телефона можно, но у этой технологии слишком много недостатков: дорого, работать в конкретный момент может только один телефон, нельзя принимать входящие звонки, могут запеленговать.

Я же реализовал другой подход, основанный на самом принципе смены ASN-пароля на сервере. В этом случае появляется возможность получать с сервера новый ASN-пароль, не стирая старый. Получается, что ASN-код будет продолжать регистрировать вас в сети, а старый пароль как бы подвисает, делая вас невидимым в сети, но при этом позволяя звонить. При этом на сервере даже не записывается ваш номер телефона и телефон получается анонимным. Звонить можно куда угодно и сколько угодно, а также отправлять SMS-сообщения.

Итак, чтобы перепрограммировать телефон, необходимо иметь шнур (MAX 232) для подключения телефона к компьютеру, получить от меня прошивку (для вашей конкретной модели телефона), которую я вышлю по электронной почте после некоторых формальностей, и затратить полчаса непосредственно на перепрограммирование (поша-

говое руководство «Как это делать» я тоже высылаю).

*Немаловажный момент: программа прошивки компилируется под каждый аппарат индивидуально (в качестве гарантии выступает IMEI-код вашего телефона или, если по-русски — серийный номер, его вы можете узнать, набрав на аппарате комбинацию кнопок *#06#). При заказе вы высылаете мне IMEI-код, модель телефона и e-mail адрес, на который будет выслана программа.*

Буквально через несколько месяцев в Сети появились десятки (!) копий этого сайта, полностью воспроизводящие не только текст (положа руку на сердце, признаем — «дурилка» составлена гениально!), но и его дизайн! Не отличались разнообразием и имена — большинство сайтов содержало в названии слово «FreeGSM». Наконец, каждый сайт был снабжен грозным предупреждением: «Этот сайт — ЕДИНСТВЕННЫЙ настоящий! Остерегайтесь подделок!», страничкой новостей и даже «работающим» форумом, заполненным хвалебными отзывами клиентов. Самые изобретательные помещали на сайты даже «демонстрационную версию» прошивки — программу-пустышку.

С владельцем «FreeGSM» сайта можно было связаться по электронной почте — при этом он охотно отвечал на любой вопрос, связанный с технической стороной проекта. Правда, послания

НАСТОЯЩИХ специалистов по технологии GSM, которые были прекрасно осведомлены о бредовости доводов в «техническом описании» и принципиальной невозможности подобной технологии взлома — «создатель» прошивки обычно предпочитал оставлять без ответа.

Если посетитель сайта выражал желание приобрести «взломанную» прошивку для своего телефона (в подробном списке на сайте обычно перечисляются все доступные в России модели телефонов), владелец сайта требовал перевести от 30 до 50 долларов «за один экземпляр прошивки» на «виртуальный кошелек в системе WebMoney». После чего связь с ним прерывалась.

Своего расцвета FreeGSM достиг в 2002–2003 годах, после чего волна пошла на убыль. Но даже сегодня сайты такого типа нет-нет да и встречаются на просторах Сети...

Официальная статистика молчит о том, сколько всего людей попалось в сети «FreeGSM». Большинство обворованных не спешило обращаться в правоохранительные органы — по вполне понятным причинам. Однако можно предположить, что число жертв махинаторов измеряется тысячами, а «улов» изобретательных дельцов — миллионами долларов.

«Генераторы карт»

После спада «Эпидемии FreeGSM» казалось, что время крупномасштабных сетевых махинаций прошло — пользователи стали куда грамотнее и, обжегшись на молоке, предпочитали дуть на воду.

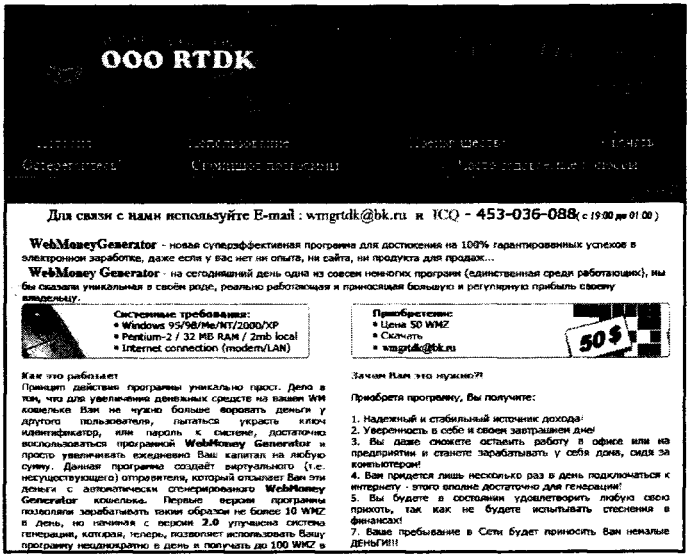
Однако, как выяснилось, базовая схема, положенная в основу мошенничества, отнюдь не утратила своей привлекательности — в 2003 году российский Интернет стал стартовой площадкой для нескольких новых афер.

На сей раз мошенники предлагали не взломанные прошивки для «мобильников», а столь же мифические «генераторы номеров» карт оплаты услуг компаний МТС, БиЛайн, а также спутникового телевидения НТВ+. Позднее их сменили столь же таинственные «генераторы» для электронных кошельков WebMoney и Яндекс.Деньги.

Обычно сайты «картоделов» содержат текст следующего типа:

!!!ВНИМАНИЕ!!!

Я создал его!!! Первый в мире ГЕНЕРАТОР ПИН-КОДОВ ДЛЯ КАРТ ОПЛАТЫ СОТОВЫХ ОПЕРАТОРОВ «PIN WRITE LIVE»: Bee Line, МТС и MEGAFON.



«Генератор» WebMoney

Программа работает следующим образом:

1. Во-первых, во время работы этой программы необходимо подключение к Интернету. (Программа работает On-line.)

2. Вы вводите пин-код любой уже активированной карты (просроченной).

3. Вводите номинал карты (вашей просроченной).

4. Нажимаете «PIN THIS», и пин-код у вас в кармане.

ВНИМАНИЕ: вы получаете только один пин-код за одну операцию, в следующий раз вы можете ввес-

ти опять же пин-код какой-нибудь просроченной карты, а можете ввести пин-код, полученный вами в ходе первой операции (но только, когда этот баланс будет израсходован!).

Срок пользования программой неограничен. Вы можете использовать ее бесконечно. И УВЕРЯЮ ВАС, эта программа не устареет, ее невозможно отследить (слишком быстро работает) и у сотовых операторов нет возможности разработать защиту против нее (такова структура программы — искусство в простоте!), так что приобретайте, пользуйтесь и не платите больше за телефоны.

Как я уже сказал, программа работает on-line, поэтому нет смысла просить пароль у тех, кто уже его купил и зарегистрировал программу — после введения оригинального пароля (в это время компьютер должен быть подключен к интернету) в папку с программой автоматически закачивается файл допуска к программе, и только тогда она начинает действовать и срок ее использования не ограничен.

Стоимость пароля — 300 рублей, для получения пароля активизации программы нужно перечислить сумму 300 рублей на кошелек WebMoney.

Возможны и вариации — например, вместо перевода денег на счет WebMoney мошенники могут требовать номера не активированных, рабочих карточек для оплаты услуг сотовой связи. В любом случае вероятность попасть на «кидалу» при

покупке «картогенераторов» приближается к стопроцентной.

Впрочем... Многим из тех, кто впервые познакомился с Сетью в начале 90-х, памятны многочисленные программы для генерации номеров кредитных карт. Многие из них являли собой банальнейший вирус... Но некоторые все же работали!

Я совершенно не исключаю, что где-то среди многочисленных сайтов-мошенников действительно отыщется реально работающий (или, вернее, работавший) генератор. Но также несомненно и то, что в случае появления такой программы алгоритм генерации номеров у НАСТОЯЩИХ карточек моментально изменился бы.

Как бы то ни было, поверьте, что попытки найти работающий генератор платежных и уж тем более кредитных карт не просто незаконны, но и заранее обречены на провал. Овчинка явно не стоит выделки...

Виртуальный «обменник»

Одна из последних афер на проверенном «движке» FreeGSM стартовала в российском сегменте Сети в конце 2003 года. На сей раз сетевые

«ловкачи» попытались проникнуть на рынок «виртуальных денег»... Где в последние годы воцарился виртуальный кавардак.

Представьте себе — сегодня в виртуальном пространстве существует добрый десяток платежных систем, каждая из которых имеет свою «сферу влияния». И, соответственно, несколько видов «киберденег».

Необходимость обменять один вид «электронной валюты» на другой возникает довольно часто — например, если вы имеете некоторую сумму в WebMoney, а ваш магазин принимает только Яндекс.Деньги. Иногда это можно сделать просто и безболезненно — с помощью сервисов самих платежных систем. Но в каждом конкретном случае надо искать специальный «обменник», универсальных пунктов существует не так уж много.

К тому же есть системы, российским пользователям пока недоступные. Например, американская система PayPal, с помощью которой можно оплатить покупки, совершенные на аукционе eBay, «скидочном» портале Half.com и сотнях других «виртуальных шопов»...

Поскольку электронными деньгами сегодня пользуются многие, то неудивительно, что нашлись желающие заработать на проблемах обладателей «виртуальной наличности»...

Сайт типа «виртуальный обменник» может предложить вам быструю конвертацию одного вида «электронной валюты» в другой, включая, естественно, лакомый PayPal, а также — быструю оплату покупок в западных Интернет-магазинах. На первый взгляд все выглядит цивильно — на сайте вы найдете солидную таблицу комиссионных (как правило, они несколько ниже официальных или равны им). Покупателям товаров на eBay предлагается выслать номер лота, адрес продавца и цену.

После первого письма клиенту высылается подробная инструкция по оплате, в которой клиенту предлагается перевести сумму авансом на «виртуальный кошелек» в WebMoney или аналогичной системе. Дальнейшее предугадать нетрудно...

«Заработок в Интернете»

Мысль о том, что не худо бы использовать возможности Сети для создания собственного — пусть маленького! — бизнеса, посещает любого неофита уже в первые часы Интернет-путешествий. Не случайно добрая треть писем, которые приходят в мой адрес от читателей, содержит один и тот же вопрос — «Как заработать деньги в Сети?».

Долгое время я вовсе не хотел касаться этого вопроса — наверное, потому, что для подробного и качественного ответа пришлось бы писать новую книжку. Однако тема ждала своего дня — и вновь всплыла на поверхность во время написания этой главы.

Ведь наряду с первым поколением мошенников, обдирающих любителей всяческой халявы, в Сети тихой сапой завелось новое поколение Остапов Бендеров. Их «клиенты» относятся к гораздо более серьезной и ответственной категории — они всерьез готовы вкладывать деньги в собственное будущее.

А, стало быть, и в информацию о том, как это самое будущее обеспечить...

Мошенничество с продажей информации — вообще один из самых излюбленных приемов российских жуликов, как в реальном, так и в виртуальном мире. Вспомним того же Остапа Бендера, с успехом продавшего недалекому репортеру Ухудшанскому состряпанный на коленке «Торжественный комплект» для сочинения передовиц на всевозможные темы. Хотя незачем клеветать на товарища Бендера — его рецепты все-таки работали, о чем неопровержимо свидетельствует вся печать советского периода.

Последователи Остапа действуют куда более грубо, но от этого не менее эффективно. Недаром

чуть ли не каждый день в столичных газетах появляются статьи о нечестных фирмах-посредниках, торгующих «липовыми» списками якобы сдающихся квартир, а разделы объявлений этих же самых газет заполнены рецептами типа «100 % рецепт быстрого заработка. Недорого».

И реальные, и виртуальные мошенники играют на одной и той же слабости — покупая информацию, мы не представляем себе, за что именно мы выкладываем свои кровные, насколько «упаковка» товара соответствует его содержанию.

Итак, вы обнаружили в Сети объявление вот такого типа:

«Уникальная авторская методика заработка в Сети!
От 1000 долларов в месяц! Интернет-трейдинг»

За рецепт обогащения обычно просят немного — от 100 рублей до 10 долларов. Не правда ли, не слишком большая цена?

Уплатив эту сумму, вы получите небольшой файл-архив, в котором, в зависимости от «профиля» продавца, может оказаться следующее:

1. Заготовка для создания типового сайта, посвященного FreeGSM или подобным аферам, с подробной инструкцией по околпачиванию простаков.

2. Архив общедоступного сайта, посвященного Forex или другой системе Интернет-торговли.

3. Совет типа «Опубликуй такое же объявление и греби бабки» (этот трюк практически в неизменном виде перешел из газетных афер еще начала 80-х годов).

Возможны и другие варианты — но даже в самом благоприятном случае вы приобретете лишь ту информацию, которую сами смогли бы найти в Сети за пару минут работы с поисковиком Яndex или Google. В общем, очередной «торжественный комплект» от фирмы «Бендер и сыновья». И придраться в данном случае будет не к чему...

Несколько более щадящим типом мошенничества являются «сетевые пирамиды», которые с успехом перекочевали из реального мира в виртуальный еще в начале 90-х годов. Поначалу они были довольно-таки безобидными, поскольку не требовали денежных вложений.

В большинстве случаев участникам пирамиды требовалось лишь читать рекламную почту (вариант — устанавливать себе на компьютер небольшую программу, демонстрирующую рекламные баннеры) — а заодно привлекать к этому высокоинтеллектуальному занятию друзей и знакомых. При этом отчисления шли как за каждое прочитанное сообщение или просмотренный баннер, так и за «новообращенных».

Второе поколение пирамид уже не выглядело таким невинным — их участники предлагали заниматься рассылкой рекламной почты (то есть попросту спама), получая доход от каждого, откликнувшегося на послание с личным номером участника.

Как и реальные системы «многоуровневого маркетинга», их виртуальные двойники позволяли заработать тем, кто оказался ближе к верху пирамиды — доходы многих участников доходили до нескольких сот долларов в месяц. Но таких счастливчиков было немного — большинство лишь теряло время, довольствуясь ежемесячным доходом в 10–20 долларов.

Сегодня мода на «рекламные пирамиды» сошла на нет (туда ей и дорога) — однако у их создателей появились достойные преемники. Сегодня в Сети вовсю процветает торговля «виртуальными акциями», обладателям которых обещаны фантастические проценты доходности (до 30–40 годовых в валюте) — при этом никакого разрешения на выпуск ценных бумаг у обладателей ресурса, естественно, нет. Вполне возможно, что для маскировки первым обладателям таких акций с помпой выплатят обещанную прибыль — но вероятнее всего, не будет и этого. Сетевые мошенники отнюдь не так озабочены безупречностью своего имиджа, как их предшественники «вне Матрицы»...

➔ Все вышесказанное не относится к солидным системам Интернет-трейдинга — например, Forex. Однако эта «виртуальная биржа», позволяющая совершать сделки с реальными ценными бумагами, может быть для новичка во сто крат более опасной, чем любой мошеннический сайт. Новичок, не обладая определенными знаниями и опытом, разорится на «честной» бирже так же легко, как и в обычном виртуальном казино...

«Музыкальная кладовая»

Семь лет назад мы обнаружили, что музыку легко выкладывать в Сеть — и добывать из нее же. Появление и распространение формата компрессии MP3 сделало явью самые сокровенные мечты меломанов... Спустя три года музыка уже составляла львиную долю сетевого трафика, а в Интернете появилось множество специализированных сайтов и сервисов, посвященных исключительно MP3-музыке. И когда пару лет назад на распространителей «музыкальной контрабанды» начались по-настоящему серьезные гонения, было уже поздно — отлаженная система просто не могла уйти в никуда.

К счастью, безнадежной (и ненужной) борьбой с пиратством дело не ограничилось. Наиболее сообразительная часть музыкальной индустрии, наконец, решилась сделать то, что нужно было предпринять с самого начала — создать систему платных музыкальных архивов. В дело пошли знаменитые в прошлом рассадники бесплатной музыки — такие, как архив MP3.Com и знаменитая файлообменная система Napster... А в начале 2003 года во весь голос заявила о себе созданная компанией Apple система ITunes, ставшая одним из самых популярных сервисов в Сети...

Но, несмотря на это, было понятно — при всем изобилии легальных «кладовых» в них все равно будет куда меньше музыки, чем в пиратских закромах... Да и вопрос цены оставался открытым — установленная такса «доллар за песню» устраивала далеко не всех. Зато легальные сайты были всегда доступны, и нужные файлы в них хранились постоянно — в отличие от пиратских «обменников»...

Словом, и у пиратов, и у «легальщиков» были свои плюсы и минусы — и все с нетерпением ожидали рождения компромиссного варианта. Хотя большинству было понятно, что компромисс тут невозможен...

И вот в конце 2002 — начале 2003 годов в Сети появилось множество странных однотипных сай-

тов, предлагающих ни много ни мало — безлимитный доступ к громадному музыкальному архиву из нескольких сот тысяч композиций! Причем некоторые сайты [например, Easy Music Download (http://easymusicdownload.com)] были снабжены и собственной поисковой системой, которая так и норовила отрыть в своем архиве десяток-другой просто невозможных раритетов! Доступ, правда, не бесплатный — но сумма в 20 долларов за годовую «подписку» выглядела чисто символической.

После перевода искомой суммы (с помощью кредитной карты) пользователь получал логин и пароль для доступа в святая святых — «закрытую» зону сайта... И вот тут-то поджидал настоящий сюрприз... в виде подборки самых обычных файлообменных программ типа Kazaa или eMule и рекомендаций по их настройке.

А чуть ниже хитрые владельцы сайта извещали ошарашенных клиентов, что свои кровные они выложили не за доступ к музыкальному архиву, а за... консультационные услуги и обучение работе с бесплатными программами! Тут же напоминалось, что при отмене аккаунта деньги на счет пользователей не возвращаются.

Только тут становилась понятна причина живучести этих сайтов — ничего противозаконного их хозяева номинально не совершали (пользователь просто не давал себе труда прочесть хорошо

запрятанный в общедоступном разделе текст «Вопросов и ответов»). А держателям легальных музыкальных архивов существование подобных «обманок» было даже на руку, благо Easy Music Download и ему подобные сайты с успехом дискредитировали всех держателей «пиратских» архивов...

ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Философы говорят, что у каждого явления в мире существуют две стороны, и светлой ипостаси всегда сопутствует темная. Не будучи философом, автор этой книги не раз убеждался в этом прискорбном факте на практике.

Конечно, это еще большой вопрос — можно ли считать то программное изобилие, которое откроется вам на страницах этой книги, однозначно «светлой» стороной (покажите нам хоть раз свет, исходящий от 100-мегабайтного текстового редактора производства небезызвестной компании!), благо и с ними проблем вполне хватает.

Но в существовании «темной стороны» уж точно сомневаться не приходится. Попробуйте сделать это хоть на миг — и злокозненные двоичные создания не преминут напомнить вам о себе.

Придется рассказать о них и нам — не просто ради того, чтобы в очередной раз пролить ложку света в темную бочку программного «подполья». Но и для того, чтобы хотя бы отчасти опровергнуть те многочисленные мифы, которые сложились вокруг вредоносных программ, путей их распространения и РЕАЛЬНОГО вреда, который они могут нанести.

А мифов этих более чем достаточно. С одной стороны, нервы пользователя меланхолично расшатывают производители антивирусных продуктов — смотрите, мол, какие кошмары могут случиться с вашей «персоналкой», ежели вы хотя бы на минутку оставите ее без нашего заботливого надзора! И рассказывают мрачные истории — да такие, что старина Хичкок наверняка умер бы от зависти (если бы не успел сделать этого раньше — по естественным причинам).

Бензина в огонь подливает телевидение, радио, печатная и электронная пресса, которые с каким-то мазохистским наслаждением раскручивают все новые и новые слухи: «В каждом компьютере сидит «программа-шпион» из ФСБ!», «Не открывайте картинки — с ними по почте приходят вирусы!», «Программа XXX кредитных карточек!»...

И уж совсем запутывают бедного пользователя, успокаивая, многочисленные друзья и знакомые — «Да брось, все это ерунда! У меня вот ни

разу вируса не было. А если и придет какой — сам об этом пожалеет»...

Программы, которые мы не выбираем...

Программы, которые всегда приходят незваными...

Программы, с которыми мы никогда, ни при каких обстоятельствах, не сможем найти общего языка...

Но знать о них все же необходимо...

Надеемся, что мы не зря посвятили вредоносным программам много страниц в этой книге. И если эта информация — в сущности, не содержащая никаких особых откровений или сенсаций, — хоть что-то прояснит в вашем сознании, мы будем считать свою задачу выполненной.

Вирусы

Ну, о вирусах, кажется, каждый из нас наслушался страшилок еще с колыбели. Пользователю-новичку порой кажется, что вирус может проникнуть в его компьютер отовсюду, чуть ли не с дуновением ветерка. А поскольку о разрушительных

последствиях его работы наслышаны все, то и страх перед вирусной атакой у начинающих пользователей порой неоправданно высок. Хотя страх этот, как мы увидим, отнюдь не мешает тому состоянию фаталистической расслабленности, в которой пребывает добрая половина пользователей. Мол, все равно не убережешься — рок, судьба, понимаете ли...

Что же это такое — компьютерные вирусы?

Прежде всего, это — САМОРАЗМНОЖАЮЩИЕСЯ ПРОГРАММЫ. Именно такое определение дал компьютерным вирусам Фрэд Коэн, один из первых исследователей этого феномена. Программы, умеющие по собственной воле, независимо от желания пользователя, создавать свои собственные копии и распространять их на другие компьютеры.

Это — одна сторона деятельности вируса. Не самая страшная, кстати. Если бы вирус просто размножался, не мешая работе программ, то с ним, наверное, не стоило бы и связываться. Тем более, что значительное число существующих вирусов принадлежит именно к этой, относительно безвредной категории.

Помимо размножения, у вируса есть еще и другое «хобби» — разрушать, пакостить. Степень «пакостности» вируса может быть разная — одни ограничиваются тем, что выводят на экран навяз-

чивую картинку, мешающую вашей работе, другие, особо не раздумывая, полностью уничтожают данные на жестком диске.

Смесь правды, полуправды и вымышленных страшилок — все, что многие из нас знают о компьютерных вирусах... А ведь такая информация — тоже своего рода вирус. «Заразившись» им, даже многие взрослые люди совершают абсолютно нелогичные поступки: бывалые компьютерщики и сегодня вспоминают «специалистов», протиравших дискеты спиртом — «для дезинфекции». Другие панически боятся устанавливать любые программы, третьи шарахаются от электронной почты... И даже установив на свой компьютер модный антивирус, такие пользователи остаются абсолютно беззащитными перед лицом настоящей опасности...

Парадоксально, но кажется, что громадное количество информации о вирусах, которое что ни день обрушивают на нас любимые СМИ, и количество мифов и предрассудков, связанных с вирусами, лишь преумножается. Причем в прямой пропорции. Вот эти-то мифы мы и постараемся развеять, дав заодно несколько советов, как застраховать себя от этой напасти. И что, собственно, она собой представляет.

Миф первый. Любой вирус способен «убить» компьютер. Если бы дела обстояли именно так, от всех компьютеров в мире давно уже ос-

тались бы информационно чистые рожки и ножки. Но, к счастью, по-настоящему «смертоносных» вирусов не так уж много: почти половина вирусного поголовья довольствуется тем, что бесконтрольно размножается и распространяет собственные клоны по другим компьютерам. Это, естественно, никоим образом не значит, что к существованию вирусов надо относиться легкомысленно — для того, чтобы устроить вам и вашему компьютеру «праздник», будет вполне достаточно одного злокозненного вируса. Недавно в сети начали распространяться вредоносные программы-«эксплоиты», использующие уязвимость системной защиты для проникновения на компьютер и уничтожения хранящейся на нем информации. И последствия такой атаки могут быть самыми непредсказуемыми...

Миф второй. Вирусы могут заражать любые файлы. В свое время вирусы действительно паразитировали на мирных программах, внедряя свой код в их тело. Однако сегодня такие экземпляры встречаются крайне редко. Чаще всего современные вирусы распространяются отдельно, маскируясь под полезную программу. Конечно, есть вирусы, поражающие определенные типы документов — например, тексты Word, электронные таблицы и т. д. Но куда большая угроза исходит от обычных электронных писем, которые могут содержать вирусную начинку, от сомнительных сайтов, напичканных вредоносными

программами-скриптами. Наконец, существуют вирусы, которые умеют проникать на незащищенный компьютер непосредственно из Сети, пользуясь «дырками» в защите операционной системы! А вот музыкальные файлы, видео или картинки вирусы поражают нечасто. Другое дело, что вирусы могут маскироваться под файлы этих типов, однако обнаружить подмену довольно просто. Как? Об этом мы подробно поговорим ниже...

Миф третий. Вирусы могут заражать электронные письма! Конечно же, в таком виде эта формулировка — абсолютный вымысел. Вирус не может заражать сами письма, которые представляют собой обычный текст. Другое дело, что вирусы распространяются через каналы электронной почты в виде ВЛОЖЕНИЙ — т. е. файлов, прикрепленных к электронному письму, либо включенных в письмо гиперссылок, щелкнув по которым, вы также можете загрузить вредоносный модуль.

Миф четвертый. Заражение компьютера наступает в момент появления в нем хотя бы одного экземпляра вируса. И это неправда — лежа на жестком диске, инфицированная программа или документ вреда вам не причинит. Активируется вирус лишь в момент запуска программы или открытия документа — никак не раньше. А потому, получив по электронной почте сомнительный файл, не паникуйте: даже в том случае, если при-

шедший к вам файл действительно заражен, вам будет достаточно просто удалить письмо с вражеской начинкой. Желательно, конечно, после этого очистить папку Удаленные вашего почтового клиента, а затем, для пущей надежности — еще и Корзину.

Наконец, миф пятый. Наличие в компьютере любых антивирусных программ — гарантированная защита от вирусов. Бесспорно, хорошая антивирусная программа — это единственный способ снизить шансы на поражение вирусом. Однако сама по себе антивирусная программа мало что может: это всего лишь оболочка, надстройка над самой важной частью — базой данных. Именно благодаря ей программа может выловить заразу, отличив ее от обычного программного файла или документа. Однако новые вирусы появляются каждый день, и если вы нерегулярно следите за обновлением базы данных вашего антивируса, вся его мощь может оказаться бесполезной. Отсюда — вывод: антивирусную базу данных необходимо обновлять не реже раза в неделю, а в идеальном случае — ежедневно. И чем чаще обновляется антивирусная база, тем надежнее вы защищены. Кроме того, сегодня одних антивирусных программ оказывается недостаточно — необходимо обновлять не только их, но и саму операционную систему, закрывая вредоносным программам путь с помощью «заплаток».

В чем же заключается реальность? А вот в чем: на самом деле вирусы — лишь верхушка айсберга. Видов вредоносных программ куда больше, и каждая из них уже давно обзавелась излюбленной лазейкой для проникновения в ваш компьютер и обладает собственным уникальным набором пакостей.

➔ Сегодня науке известно около 50 тысяч компьютерных вирусов — маленьких вредоносных программок, следующих в своей жизни только трем заповедям — Плодиться, Прятаться и Портить. И бороться с ними необходимо по-разному, поскольку универсального средства, увы, не существует...

Классифицировать вирусы можно по-разному — по их «биологическому виду», либо — по способу распространения. Совершенно не обязательно знакомиться с представителями всех групп в рамках этой книги — тем более, что в Сети уже давно существует великолепная вирусная энциклопедия, созданная «Лабораторией Касперского» (http://www.viruslist.com/index.html). Назовем лишь несколько наиболее важных групп.

⏭ Условно и наиболее грубо вирусы можно разделить на **программные** и **скриптовые**. Вирусы первой группы представляют собой отдельные и автономные саморазмножающиеся программы, часто снабженные еще и деструктивной, разрушительной функцией. «Скриптовые» виру-

сы, напротив, являются не отдельными программами, а набором инструкций для какой-либо из популярных программ Windows (Internet Explorer, программы Microsoft Office, Windows Media Player).

Что же касается типа распространения, то подавляющее большинство самых вредоносных сегодняшних вирусов относятся к типу **«Интернет-червей»**, которые распространяются преимущественно в виде файлов-вложений в электронные письма.

Другими, чуть менее популярными каналами распространения вирусов являются сети каналов IRC (Internet Relay Cat), а также системы обмена файлами типа Kazaa, SoulSeek, EDonkey и ряда других. Правда, пользователей этих систем в России гораздо меньше, чем обладателей адресов электронной почты, поэтому в отдельные группы эти вирусы обычно не выделяют. Да и тактика вирусов в этих случаях не слишком отличается от обычной — они либо маскируются под файлы других типов (картинки, музыка и т. д.) с помощью «двойного расширения», либо, напротив, выдают себя за полезные программы.

Классические вирусы-«паразиты»

...А началась эта история ни много ни мало — лет тридцать назад. Именно тогда, в конце 60-х, когда о «персоналках» можно было прочитать лишь в фантастических романах, в нескольких «больших» компьютерах, располагавшихся в крупных исследовательских центрах США, обнаружились очень необычные программы. В отличие от программ нормальных, послушно «ходивших по струнке» и выполнявших все распоряжения человека, эти гуляли сами по себе, подобно киплинговской кошке. Занимались в недрах компьютера какими-то понятными только им делами, по ходу дела сильно замедляя работу компьютера. Хорошо хоть, что ничего при этом не портили и не размножались.

Однако продлилось это недолго. Уже в 70-х годах были зарегистрированы первые настоящие вирусы, способные к размножению и даже получившие собственные имена: большой компьютер Univac 1108 «заболел» вирусом Pervading Animal, а на компьютерах из славного семейства IBM-360/370 свил гнездо вирус Christmas tree.

К 1980-м годам число активных вирусов измерялось уже сотнями. А появление и распростране-

ние персональных компьютеров породило настоящую эпидемию — счет вирусов пошел на тысячи. Правда, термин «компьютерный вирус» появился только в 1984 году: впервые его использовал в своем докладе на конференции по информационной безопасности сотрудник Лехайского Университета США Ф. Коэн.

Первые «персоналочные» вирусы были существами простыми и неприхотливыми — особо от пользователей не скрывались, «скрашивали» свое разрушительное действие (удаление файлов, разрушение логической структуры диска) выводимыми на экран картинками и каверзными «шутками»: «Назовите точную высоту горы Килиманджаро в миллиметрах! При введении неправильного ответа все данные на вашем винчестере будут уничтожены!!!». Выявить такие вирусы было нетрудно: они «приклеивались» к исполняемым (*.com или *.exe) файлам, изменяя их оригинальные размеры, — чем и пользовались первые антивирусы, успешно выявлявшие нахалов.

Забавно, что первые вирусы этого типа были созданы в качестве... средства борьбы с пиратами: в 1985 году десятки тысяч компьютеров по всему миру оказались заражены вирусом Brain, разработанным братьями-пакистанцами Алви. Как выяснилось, хитрые пакистанцы, владевшие собственным программным бизнесом, умышленно начиняли свой товар вредоносной начинкой,

срабатывавшей только при установке на компьютер нелегальной копии.

За десять лет, прошедших с момента появления «пакистанского» вируса, его потомки сумели распространиться по всему миру. Их опасность заключалась в том, что такие вирусы могли укрыться в абсолютно любой программе — точнее, в ее главном, исполняемом файле. Достаточно было одного-единственного запуска программы, чтобы вирус проник на компьютер и начинал активно заражать все остальные файлы с расширениями com и exe.

➔ «Золотой век» классических вирусов продолжался около десяти лет — сегодня их поголовье резко сократилось и, по оценкам Лаборатории Касперского, составляет не более нескольких процентов от всех вирусов. Бороться с ними умеет любой современный антивирус, да и сама операционная система неплохо защищена от их атак. Некоторые типы вирусов — такие как «boot-вирусы», поражающие загрузочный сектор жесткого диска, сегодня практически истреблены.

Казалось, фантазия вирусописателей наконец-то истощилась. И когда против stealth-вирусов было наконец-то найдено «противоядие», компьютерный народ вздохнул с облегчением. А все еще только начиналось...

Вирусы-программы (W32)

Со временем вирусы, прятавшие свой код в теле других программ, сдали свои позиции. Во многом это произошло из-за того, что размеры самих вирусов стали больше — а спрятать код размером в сотни килобайт не так-то просто. Да и сами программы и операционные системы резко поумнели, научившись проверять целостность собственных файлов.

В итоге произошло то, что и должно было случиться — «исполняемые» вирусы перестали маскироваться, представ перед публикой в «чистом» виде. Вирус превратился в абсолютно отдельную, независимую программу, не нуждающуюся в «хозяине-переносчике». Однако сразу же перед вирусописателями встал другой вопрос — а как заставить пользователей скачать и запустить у себя на машине этот самый вирус?

«Программные» вирусы, написанные для операционной системы Windows, решили эту проблему, маскируясь под разные «полезные» утилиты — например, под «ломалки» для условно-бесплатных программ или мультимедийные презентации. Другой излюбленный прием распространителей заразы — наряжать свои детища в «одежду» об-

новлений для операционной системы или даже... антивирусной программы! Увы, до сих пор многие пользователи, не задумываясь, запускают неизвестные программы, пришедшие в виде вложения в электронные письма якобы от Microsoft или «Лаборатории Касперского» — а ведь это самый верный путь поселить на свой компьютер злокозненного паразита!

Большинство вирусов люди запускают на своем компьютере самостоятельно! — увы, несмотря на все усилия борцов с вирусами, некие стереотипы человеческой психологии оказываются непреодолимыми...

В 1995–1999 годах на просторах Интернета весело резвилась добрая сотня «Windows-совместимых» вирусов. Эти милые зверушки, понятно, резвились не просто так... Только за период лета 1998 — лета 1999 года мир пережил несколько поистине разрушительных вирусных атак: в результате деятельности вируса Win95.CIH, поражающего BIOS системной платы, из строя были выведены около миллиона компьютеров во всех странах мира.

А в середине 2003 года Сеть оказалась поражена новым «червем» SoBig, распространявшимся в виде вложения в электронные письма. Несмотря на то, что о вредоносных «вложениях» уже давно трубила вся пресса, люди запускали файл-вирус без малейших опасений.

Впрочем, некоторые вирусы способны атаковать ваш компьютер даже в том случае, если его «тело» физически находится в другом месте. Например, один из самых «модных» вирусов 2003 года — Blaster — был способен атаковать все компьютеры в локальной сети с одной-единственной машины! Сканируя локальную сеть, программа обнаруживала бреши в защите каждого компьютера и самостоятельно пропихивала в эту «дырочку» вредоносный код.

Для борьбы с W32-вирусами одной антивирусной программы, увы, недостаточно — главным условием вашей безопасности является обязательная и регулярная загрузка дополнений к Windows. А именно — файлов-«заплаток», предназначенных для закрытия уже обнаруженных «дыр» в системе защиты операционной системы.

Для получения новых «заплаток» вам необходимо навестить центр обновления Windows — сайт Windows Update (http://windowsupdate.microsoft.com). При этом совершенно необязательно набирать этот адрес в строке браузера вручную — достаточно зайти в меню ***Сервис*** программы Internet Explorer и выбрать пункт ***Windows Update***.

На открывшейся страничке вы увидите полный список обновлений, доступных для загрузки. Учтите — все обновления из раздела ***Критические***

обновления необходимо устанавливать в обязательном порядке!

Посещайте сайт Windows Update не реже раза в месяц, регулярно обновляйте базы данных вашего антивирусного пакета — и можете считать, что от львиной доли неприятностей вы застрахованы....

Макровирусы

В эпоху «классических» вирусов любой более-менее грамотный пользователь прекрасно знал: источником вирусной заразы могут быть только программы. И уж вряд ли даже в страшном сне могло присниться, что через несколько лет смертоносной начинкой обзаведутся... текстовые документы! Впрочем, такие сообщения время от времени проскакивали еще в конце 80-х годов. Но появлялись они преимущественно первого апреля, так что никакой реакции, кроме смеха, вызвать не могли.

Как оказалось, смеялись напрасно...

В 1995 году после появления операционной системы Windows 95 Microsoft с большой помпой объявила: старым DOS-вирусам конец, Windows защищена от них на 100 процентов, ну

а новых вирусов в ближайшее время не предвидится. Если бы! Уже в том же 1995 году было зарегистрировано несколько мощных вирусных атак и создан первый вирус, работающий под Windows 95.

А меньше чем через полгода человечество было огорошено вирусами нового, совершенно неизвестного типа и принципа действия. В отличие от всех «приличных» вирусов, новички паразитировали не на исполняемых файлах, а на документах, подготовленных в популярных программах из комплекта Microsoft Office.

Ларчик открывался просто: в текстовый редактор Microsoft Word и в табличный редактор Microsoft Excel был встроен свой собственный язык программирования — Visual Basic for Applications (VBA), предназначенный для создания специальных дополнений к редакторам — макросов. Эти макросы сохранялись в теле документов Microsoft Office и легко могли быть заменены вирусами. После открытия зараженного файла вирус активировался и заражал все документы Microsoft Office на вашем диске.

Первоначально макровирусы — а именно так назвали новый класс вирусов, — вели себя довольно пристойно. В крайнем случае — портили текстовые документы. Однако уже в скором времени они перешли к своим обычным обязанностям — уничтожению информации.

К такому повороту дел борцы с вирусами явно не были готовы. И потому буквально через несколько дней после своего появления вирус Concept, поражающий документы Word, распространился по всей планете. Зараженные файлы Word с лакомым содержанием (например, списками паролей к Интернет-серверам с коллекциями порнографических картинок) путешествовали от пользователя к пользователю через Интернет. Доверчивые пользователи хватали «наживку» не задумываясь — ведь даже самые умные из них с молоком матери впитали тезис: через тексты вирусы не передаются! В итоге за четыре года, прошедших с момента появления первого «макровируса», этот класс вирусов стал самым многочисленным и опасным.

Одна из самых мощных атак макровирусов была зарегистрирована в марте 1999 года, когда вирус Melissa, созданный программистом Дэвидом Смитом, всего за несколько часов распространился по всему миру. И хотя этот вирус был сравнительно безопасным (Melissa ограничивалась тем, что заражала все существующие документы и рассылала свои копии людям, внесенным в адресную книгу Microsoft Outlook), его появление наделало немало шума.

Именно появление Melissa заставило Microsoft срочно оснастить программы Microsoft Office защитой от запуска макросов. При открытии любого документа, содержащего встроенные

макросы, умный Word или Excel обязательно спросит пользователя: а вы уверены, гражданин хороший, что вместо всяческих полезностей вам не подсовывают в документе всяческую бяку? И стоит ли эти макросы загружать? Нажмите кнопку ***Нет*** — и вирусу будет поставлен надежный заслон. Просто удивительно, что, несмотря на такую простоту защиты, большинство пользователей игнорирует предупреждения программы. И заражаются...

«Майка лидера» принадлежала макровирусам около пяти лет — срок, по меркам компьютерного мира, немалый. Выжить и преуспеть им помог Интернет — в течение последних лет вирусы этого типа распространялись в основном по электронной почте. Источником заражения мог быть и присланный компьютерной фирмой прайс-лист, и рассказик, отосланный в виде файла-вложения незадачливым другом.

Сегодня число макровирусов снизилось в несколько раз — им принадлежит не более 15 процентов всего вирусного «рынка». Однако опасность заражения макровирусами по-прежнему высока — и поэтому будьте особенно осторожны, если вам часто приходится иметь дело с документами, созданными на других компьютерах. Качественный антивирус в сочетании с вклю-

ченной защитой от макросов в программах Microsoft Office могут надежно обезопасить вас от подобной напасти.

Скрипт-вирусы

На самом деле макровирусы, описанные в предыдущей главе, являются не самостоятельным «видом», а всего лишь одной из разновидностей большого семейства вредоносных программ — скрипт-вирусов. Их обособление связано разве что с тем фактом, что именно макровирусы и положили начало всему этому семейству, к тому же вирусы, «заточенные» под программы Microsoft Office, получили наибольшее распространение из всего клана.

Общая черта скрипт-вирусов — это привязка к одному из «встроенных» языков программирования. Каждый из них привязан к конкретной «дырке» в защите одной из программ Windows и представляет собой не самостоятельную программу, а набор инструкций, которые заставляют в общем-то безобидный «движок» программы совершать несвойственные ему разрушительные действия.

С конца 1990-х годов скрипт-вирусы сумели «оседлать» великое множество программ. Помимо уже знакомого семейства «макровирусов»

встречаются «зверушки», умеющие атаковать Internet Explorer или Windows Media Player различных модификаций.

Как и в случае с документами Word, само по себе использование микропрограмм (скриптов, Java-апплетов и т. д.) не является криминалом, — большинство из них вполне мирно трудится, делая страничку более привлекательной для глаза или более удобной. Чат, гостевая книга, система голосования, счетчик — всем этим удобством наши странички обязаны микропрограммам-«скриптам». Что же касается Java-апплетов, то их присутствие на страничке тоже обосновано — они позволяют, например, вывести на экран удобное и функциональное меню, которое разворачивается под курсором вашей мышки...

Удобства удобствами, но не стоит забывать, все эти апплеты и скрипты — самые настоящие, полноценные программы. Причем многие из них запускаются и работают не где-то там, «в прекрасном далеке», на неведомом сервере, а непосредственно на вашем компьютере! И, встроив в них вредоносную начинку, создатели страницы смогут получить доступ к содержимому вашего жесткого диска. Последствия уже известны — от простой кражи пароля до форматирования жесткого диска.

Разумеется, со «скриптами-убийцами» вам придется сталкиваться во сто крат реже, чем с

обычными вирусами. Кстати, на обычные антивирусы в этом случае надежды мало, однако открытая вместе со страничкой зловредная программа должна будет преодолеть защиту самого браузера, создатели которого прекрасно осведомлены о подобных штучках.

Вернемся на минутку к настройкам Internet Explorer — а именно в меню ***Сервис*** ▸ ***Свойства обозревателя*** ▸ ***Безопасность***.

Как видим, Internet Explorer предлагает нам несколько уровней безопасности. Помимо стандартного уровня защиты (зона ***Интернет***) мы можем усилить (зона ***Ограничить***) или ослабить свою бдительность (зона ***Надежные узлы***). Нажав же кнопку ***Другой***, мы можем вручную отрегулировать защиту браузера, разрешив или запретив работу различных «активных элементов» страничек.

Хотя в системе безопасности того же Internet Explorer полно «дырок», которыми и могут воспользоваться злоумышленники, при грамотном использовании вы застрахуете себя от большинства неприятных неожиданностей. Скажем, входя на сомнительный «хакерский» сайт, защиту можно и усилить...

Впрочем, большая часть скрипт-вирусов распространяется через электронную почту (напомним, что такие вирусы чаще всего называют

«Интернет-червями»). Пожалуй, ярчайшими представителями этого семейства являются вирусы LoveLetter и Anna Kournikova, атаки которых пришлись на сезон 2001–2002 года. Оба этих «зверька» использовали один и тот же прием, основанный не только на слабой защите операционной системы, но и на наивности пользователей.

Мы помним, что переносчиками вирусов в большинстве случаев являются сообщения электронной почты, содержащие вложенные файлы. Помним и то, что зараза может проникнуть в компьютер либо через программы (то есть исполняемые файлы с расширением *.exe или *.com), либо через документы Microsoft Office, которые могут содержать вредоносные участки кода. Нам также известно, что со стороны картинок или звуковых файлов никакая неприятность грозить вроде бы не может. А потому, раскопав нежданно-негаданно в почтовом ящике письмо с прикрепленной к нему (судя по имени файла и расширению) картинкой, тут же радостно ее запускаем... И обнаруживаем, что под личиной картинки скрывался вредоносный вирусный «скрипт». Хорошо еще, если обнаруживаем сразу, а не после того, как вирус успел полностью уничтожить все ваши данные.

Хитрость создателей вируса проста — файл, который показался нам картинкой, имел двойное расширение! Например

AnnaCournikova.jpg.vbs

Вот именно второе расширение и является истинным типом файла, в то время как первое — просто часть его имени. А поскольку расширение *vbs* Windows хорошо знакомо, она, не долго думая, прячет его от глаз пользователей, оставляя на экране лишь имя

AnnaCournikova.jpg

Именно так Windows поступает со всеми зарегистрированными типами файлов: разрешение отбрасывается, а о типе файла должен свидетельствовать его значок. На который, увы, мы редко обращаем внимание.

Хороша ловушка?

Хороша. Но различить ее легче легкого: фокус с «двойным расширением» не проходит, если мы заранее активируем режим отображения типов файлов. Сделать это можно с помощью меню ***Свойства папки*** на Панели управления Windows: щелкните по этому значку, затем откройте закладку ***Вид*** и **снимите** галочку со строчки ***Скрывать расширения для зарегистрированных типов файлов***.

Впрочем, совершенно не обязательно, что вирусы сочтут нужным маскироваться. Иногда exe-файлы «вложены» в письмо совершенно от-

крыто. И, казалось бы, тут уже и дураку понятно, что речь идет о вирусной атаке (особенно если письмо пришло от незнакомого вам человека). Однако и эти программы с охотой запускаются пользователями: одним из них коварные вирусописатели обещают продемонстрировать неизъяснимой красоты картинки (что, кстати, и делают), другим сулят программу для «взлома» Интернета, третьим представляются обновлением к популярной программе. Способов запудрить пользователю мозги немало. А ведь бывает и так, что зараженный файл со спокойной совестью посылает вам друг или знакомый... Наконец, вирусы вы можете заполучить вместе с самими программами — особенно в том случае, если вы скачиваете их с неизвестных вам серверов.

ЗАПОМНИТЕ: в качестве «вложения» в письмо допустимы лишь несколько типов файлов. Относительно безопасны (если не считать фокусов с «двойным расширением») файлы txt, jpg, gif, bmp, tif, mp3, wma. «Условно-съедобными» можно признать документы Microsoft Office (doc, xls) и архивы zip и rar. Они, конечно, могут содержать вирус, но его вполне можно нейтрализовать с помощью антивирусной программы, при условии, что вы регулярно обновляете ее базы. Во всяком случае, такой файл можно открыть для просмотра.

А вот список безусловно опасных типов файлов: найдя их в присланном вам электронном письме, смело отправляйте его в мусорную корзину... которую потом стоит еще и очистить.

- asx
- bas
- bat
- cmd
- com
- cpl
- crt
- exe
- inf
- ins
- js
- msc
- msi
- pif
- reg
- scf
- scr
- shs
- vbs

Сами по себе эти файлы — создания вполне мирные, так что не стоит лихорадочно шерстить компьютер, удаляя их направо и налево. Нет: знаком опасности является только присутствие этих файлов в письме, поскольку каждый из них почти наверняка несет в себе вирусную начинку.

Список потенциальных «вирусоносителей» включает еще не один десяток типов файлов. Но эти встречаются чаще других.

«Троянские» программы и руткиты

В последние несколько лет наряду с уже хорошо знакомой нам вирусной угрозой стали говорить об опасности, исходящей от программ другого типа — программ-«троянцев». Распространяются они через те же каналы, что и вирусы: «троянец» может нанести вам визит в виде вложения в электронное письмо, просочиться через защиту браузера или обосноваться в дистрибутивном комплекте скачанной вами программы.

Название «троян» или «троянец» пришло еще из ДОСовых времен, куда в свою очередь — из известного античного романа о мытарствах деревянной лошади, которую по глупости притащили в одноименный город.

Изначально под троянами подразумевались программы, которые помимо своей основной работы решали еще какую-то скрытую от взора пользователя задачу. Классическим примером троянца можно считать неоднократно описанную в различных (полу)фантастических рассказах ситуацию, когда какая-то корпоративная программа, не обнаружив в платежной ведомости фамилию программиста, ее написавшего, начинала всячески «шалить».

В старые времена трояны писались именно как некие дополнительные функции какой-то основной программы. Например, один мой знакомый, чтобы получить привилегированный доступ в университетскую машину, в свое время написал игрушку по мотивам «Пикника» Стругацких, которая в процессе игры имитировала сбой, выводила окно для входа в систему и сохраняла введенный пароль в файл.

Сегодняшние «троянцы» чаще всего занимаются тем, что **воруют пароли** для доступа в Интернет и другую «секретную» информацию (например, номера кредитных карточек) и пересылают ее «хозяину». (А как вы думаете, откуда на «хакерских» сайтах берутся пароли для бесплатного подключения и номера кредиток?). Такими же темными делами занимаются и «кейлоггеры» — программки, которые втихаря отсылают своему автору информацию о том, по каким именно клавишам вы щелкали в течение всего дня. Нетрудно догадаться, что из этой текстовой мешанины можно легко выудить и номера кредиток, и пароли к сайтам или почтовому ящику.

Другой распространенный вариант — это **установка различных серверов для удаленного управления** и открытие «черных ходов» для доступа к вашей системе. Этим занимаются самые опасные разновидности вредительских программ — «руткиты», «трояны-невидимки», кото-

рые умеют так хитро маскироваться в системе, что обнаружить их присутствие фактически невозможно. Если подобный «зверь» оказался у вас в системе, то его хозяин сможет работать на вашем компьютере почти как на своем собственном.

Существуют и другие виды руткитов, которые могут, к примеру, **заблокировать на вашем компьютере запуск определенных программ**. В распространении подобной заразы была уличена даже компания Sony: в 2005 году в музыкальном мире разразился грандиозный скандал после того, как на выпущенных этой компанией «защищенных от копирования» CD была найдена программа-руткит. Мелкая тварь незаметно устанавливалась на компьютер в момент загрузки диска и препятствовала его копированию — а заодно и нарушала работу всей системы. Вал исков заставил Sony признать свою вину и изъять из продажи все зараженные CD... Но кто знает, не последовал ли кто-то ее примеру? Ведь руткиты тем и опасны, что их практически невозможно обнаружить.

Как «трояны» и руткиты попадают на компьютер? К сожалению, однозначно тут сказать ничего нельзя... Чаще всего заражение происходит, когда пользователь запускает какую-то программу, полученную из «сомнительного источника».

Стандартным способом распространения троянов является рассылка **писем от имени известных серверов**, причем в письме указывается, что прицепленный файл — это новая программа/ заплатка и т. п.

Другой способ — **письмо, якобы по ошибке попавшее не туда**. Основная задача таких писем — заинтересовать вас и заставить запустить прицепленный файл. Учтите, что даже прицепленная картинка может оказаться троянцем: можно, например, назвать его «1.gif много пробелов.exe» и прицепить соответствующую иконку — и вы в своей почтовой программе увидите только кусок названия: «1.gif».

Не менее распространенной является **маскировка «троянцев» под новые версии известных программ** (в том числе антивирусов) и под... троянцев. Так что, если вы решите поразвлечься и подсунуть «трояна» своему знакомому, то не исключено, что и сами окажетесь жертвой злоумышленника.

Бывает и по-другому — к примеру, заходите вы на «хакерский» сайт с ломалками-«крэками» для популярных программ. И тут вам ненавязчиво предлагают загрузить какой-то наворочченный download-менеджер — мол, ничем другим программки с сайта утянуть нельзя. Вы покупаетесь — и получаете вместо «качалки»

(или вместе с ней) распрекраснейший экземпляр троянской программы!

Общее правило: всегда с подозрением относитесь к файлам, полученным из незнакомого источника. Да и из знакомого — тоже. Любой файл, полученный вами по почте, если вы заранее не договаривались о его отправке вам, скорее всего, окажется трояном. Большинство так называемых «хакерских» программ, предназначенных для взлома сети и т. п. — тоже окажутся «троянами». Здесь очень хорошо срабатывает правило: «То, что у вас паранойя, еще не значит, что за вами не следят».

Кстати, довольно часто «троянца» можно определить и по стилю письма. Если вы получаете письмо или видите на страничке что-то вроде «эй, чувак, здесь самая крутая нюка», то процентов 90, что это именно троян.

Для того чтобы «троян» мог творить свое «черное дело», он должен быть запущен у вас на компьютере. В первый раз вы запускаете его сами, но надеяться на то, что вы будете делать это каждый раз — нельзя. Соответственно, троянец должен позаботиться о том, чтобы не умереть после перезагрузки компьютера.

В Windows есть три места, откуда программа может автоматически запуститься при загрузке системы: папка ***Автозагрузка***, win.ini и реестр (разумеется, есть еще различные драйверы, но такие сложные «трояны» встречаются очень редко). Так что, если вы будете периодически проверять эти места, скажем, с помощью PC Security Guard или RunServices, на предмет «неопознанных» программ, то с большой долей уверенности сможете обезвредить троянов.

Другое дело, что надо еще разобраться, что это именно «троян»... Дело в том, что в Windows живет огромное количество файлов, и определить, должен ли этот файл здесь «жить» или это «пришелец», довольно сложно. Тем более что многие трояны имеют достаточно правдоподобные названия, например browser.exe или spoolsrv.exe...

Уже запущенного «трояна» определить сложнее, хотя тоже возможно. Нажав ***Ctrl-Alt-Del*** или используя какую-нибудь специальную программу, можно посмотреть список процессов, запущенных на вашем компьютере. С помощью утилиты netstat (или другой аналогичной) можно посмотреть, с кем и на каком порту ваш компьютер устанавливает связь. Правда, для пользования этими утилитами (точнее, для того, чтобы понять их результаты) требуются определенные знания...

Кстати, косвенным признаком наличия «трояна» может служить Интернет-активность

вашего компьютера в то время, когда вы ничего не делаете (хотя, с тем же успехом, это может оказаться какая-нибудь безобидная утилита, проверяющая в фоновом режиме ваши закладки или кеширующая страницы).

Ну и, наконец, традиционный способ: антивирусы. К сожалению, до последнего времени большинство из них боролось именно с вирусами, отлавливая некоторых «троянцев» в качестве побочного результата. На мой взгляд, лучшие результаты здесь показывает AntiViral Toolkit Pro — его база «троянов» достаточно велика и включает наиболее распространенные из них.

Даже если вы вычислили «троянца», то не факт, что вам удастся его легко удалить — Windows не разрешает удалять файлы запущенных программ. Поэтому вам надо определить, откуда запускается «троянец», удалить эту запись, перезагрузить компьютер и уже после этого убить вредный файл. Хотя, лучше его не убивать, а для начала куда-нибудь переместить — вдруг это все-таки что-то нужное...

Еще один способ — блокирование связи «трояна» с автором. Большинство современных «троянов» «рассчитано» на Интернет, поэтому здесь вам понадобится файрволл (firewall). **Файрволл** — это такая специальная программа, которая пропускает «разрешенные» данные и не пропускает «неразрешенные». Установка и настройка профессиональ-

ного файрволла — дело достаточно сложное и требующее изрядных знаний о том, как что работает, но существуют и более простые версии, рассчитанные на относительно начинающих пользователей.

При каждой попытке какой-либо программы связаться с Интернетом файрволл будет спрашивать, санкционировано это соединение или нет. Разумеется, вы сможете «запомнить» разрешения для каждой программы, чтобы не отвечать на вопросы каждый раз, когда пытаетесь скачать почту.

Немножко о том, как предотвратить появление «троянов». Тут следует помнить две вещи: во-первых, то, что усиление защиты всегда ведет к некоторым неудобствам в работе (дополнительные пароли, шифрование, проверка логов, большая загрузка компьютера и т. п.), а во-вторых, замечательное правило «90/10» — «90 процентов работы требуют 10 процентов времени. Оставшиеся 10 процентов работы требуют 90 процентов времени». Работает это правило и в защите — серия элементарных мер безопасности защитит вас от 90 процентов атак.

Итак, следует принять за правило:

Любой файл, полученный из сети, если вы заранее не договаривались о его отправке, **может оказаться «трояном»**. Даже вполне безо-

бидный файл, скажем, картинка — она может быть замаскированной программой. Каждый такой файл надо либо сразу удалить, если он вам не нужен, либо сохранить на диске и проверить антивирусом, а заодно и посмотреть, что он собой представляет. Например, щелкнуть по нему правой кнопкой мыши и выбрать пункт Свойства.

Любую новую программу стоит запускать с включенным антивирусом и файрволлом, а если увидите, что она пытается связаться с Интернетом, то проводить более детальную проверку. Перед запуском и после него надо сравнить список автоматически запускаемых программ — «троян» может не запускаться сразу, а только прописать себя, скажем, в реестре и запуститься после перезагрузки. Для отслеживания подобных действий удобно использовать программу Jammer — она предупредит, что какая-то программа пытается что-то записать в автозагрузку.

Ну и, наконец, надо запомнить, что **ни одна сравнительно известная организация не рассылает никаких программ в виде почтовых вложений.**

«Шпионские» программы и рекламные модули

Нет, это не вирусы — хотя по злокозненности наши «герои» схожи с этой заразой: вашей информации повредить они не могут, а вот по назойливости им равных нет. «Шпионские» и рекламные модули, которые втихаря снабжают своих создателей информацией о вашей работе — а заодно и «подкармливают» вас изрядной порцией ненавязчивых (а иногда — и ОЧЕНЬ даже навязчивых) советов и заманчивых предложений.

Как это может произойти? Да элементарно: к примеру, заходите вы на незнакомый сайт, который тут же предлагает вам АБСОЛЮТНО БЕСПЛАТНО установить на компьютер программу для вставки в письма и сообщения вашей «аськи» крутейших анимированных смайликов. Выглядят они действительно очень круто: катаются по экрану, подмигивают, строят рожицы и даже порой издают какие-то звуки. Прикольно!

Вы щелкаете на кнопку ***Установить*** — и действительно, искомые смайлики скачиваются и устанавливаются, и ваш антивирус молчит как партизан... Все вроде бы нормально! Отнюдь: через несколько минут вы замечаете, что проклятые

смешинки заставляют ваш браузер при каждом открытии заходить на их сайт, который тут же начинает засыпать вас рекламой. Вы меняете страничку — и все равно после перезагрузки все возвращается на круги своя. Убить эту заразу нет никакой возможности, как удалить ее — неизвестно...

Точно такая же история может произойти, если вы когда-то — чисто случайно — зашли на какой-то хитрый порносайт, который тут же прописал себя во всех возможных настройках вашей операционной системы. Наконец, рекламную начинку нетрудно подцепить вместе с какой-нибудь условно-бесплатной (или бесплатной) программой. Например, рекламными добавками напичкана даже всеобщая любимица ICQ — хорошо еще, что в настройки браузера она не лезет, а рекламу показывает лишь в своем собственном окне.

Те самые «смайлики»

Подобные неприятности могут подстерегать вас на сайтах Интерент-казино, на сайтах с коллекциями «бесплатных» картинок и т. д.

Чтобы вам не пришлось горько сожалеть о последствиях одного-единственного

щелчка мышью, соблюдайте одно простое правило.

Никогда, ни при каких обстоятельствах не соглашайтесь на установку неизвестных программ и модулей ActiveX, даже если сайт настоятельно рекомендует вам сделать это! Неважно, что предлагается — хитрый «вьювер» для картинок или продвинутый поисковый «плагин»... Как правило, таким образом на вашу машину пролезают совершенно другие программы, избавиться от которых будет трудно.

Но это все реклама: надоедливо, противно, но вроде бы безопасно. А вот «шпионские» модули (spyware) — штука куда более неприятная. Такой вот «шпионский» модуль — это тот же «троянец», но не «дикий», а прирученный и окультуренный хозяином того или иного сайта или разработчиком программы. Вреда от него вроде бы и нет, но... согласитесь, не очень приятно осознавать, что за тобой постоянно наблюдает недремлющее око Большого Брата. Или даже сотни глаз маленьких, но очень навязчивых «братцев»...

Что ж, информация о программах-«шпионах» имеет под собой некую реальную почву. Громадное количество сегодняшних утилит буквально напичкано всевозможной «следяще-фиксирующей» начинкой, которая мало того, что фиксирует действия пользователей, но и что-то там передает «на сторону». Точнее — своему собствен-

ному создателю. Только не надо думать, что дело ограничивается отдельными программами — о какой «приватности» может идти речь, когда шпионским содержимым напичкана Самая Главная Программа на вашем компьютере — операционная система? Не случайно ведь последние версии Windows так привязаны к Интернету, что без подключения к Сети работа с ними становится, мягко скажем, не слишком удобной...

Однако на деле все оказывается далеко не так страшно и не так опасно, как любят представлять некоторые излишне ретивые защитники приватности...

Безусловно, большинство тех же adware-программ не только радует наш взор рекламными баннерами, но и поддерживает «обратную связь» с разработчиком — надо же ему как-то отслеживать результаты собственных усилий? Самым популярным видом «шпионства» является отсылка разработчику информации о том, на какие именно рекламные баннеры в программе вы «купились», обозначив свой интерес щелчком мыши по заветной картинке. В дальнейшем это позволит поставщикам рекламы скорректировать ассортимент скармливаемой вам рекламной массы. Щелкнули вы разок по изображению кроссовок — будьте уверены, что в дальнейшем реклама спорттоваров будет возникать перед вашими очами гораздо чаще.

Идем дальше. Допустим, программа начинает наглеть и шпионить не только за собственными рекламными окошками, но и за тем, какие странички вы открываете в браузере (нечто подобное творит, например, популярная программа для хранения паролей Gator). Вот это уже не слишком приятно — хотя и реальной опасности также не представляет. Ведь в данном случае вся собранная информация идет не к спецслужбам и не к злой Пульхерии Никитишне Штангенциркуль из Комиссии по Защите Сетевой Морали. А все к тем же рекламщикам. Хотя и это тоже не слишком приятно.

Но больше всего человек начинает беспокоиться после того, как обнаруживает возможность утечки самого дорогого — того, что именуется «персональной» информацией. То бишь милых сердцу фамилии-имени-отчества, электронного адреса... и прочей мелкой ерунды, которую каждый человек наивно считает своей главной магической тайной.

Это может произойти как явным порядком (например, при бесплатной регистрации программы, связанной с заполнением некоей «формы»), так и неявным — программа отсылает искомое «тихой сапой».

Конечно, мало кто любит сообщать какие-то личные данные о себе. Необходимость сделать это при регистрации чего-либо, будь то доменное

имя, программа или что-то еще, вызывает глухое чувство не то чтобы негодования, но раздражения. И это раздражение выливается в, пожалуй, страх того, что его данные будут куда-то переданы, — и именно в негодование, в том случае, если они действительно были переданы. Особенно, если эта передача происходила без ведома самого «объекта». Однако помните, что это — МАКСИМУМ того, что может позволить себе честная «рекламно-оплачиваемая» программа, «шпионская» начинка которой сработана серьезной компанией. Если же коварная «софтина» решится на большее — например, на несанкционированную отсылку номера кредитной карточки — она тут же переходит в статус *«трояна»* — со всеми вытекающими отсюда последствиями. И будьте уверены — никто из солидных фирм на такой фокус не пойдет.

Лучшие средства защиты

Ну что ж, теперь, когда мы узнали врага в лицо, время выбирать надежные «доспехи»! Полностью «отсечь» вирусы от вашего компьютера вряд ли удастся, разве что вы удалите из системы дисковод, перестанете работать в Интернете и будете пользоваться только легальным программным

обеспечением. Но в наших условиях все эти советы — особенно последний — выглядят либо утопией, либо издевательством.

Остается один способ: снабдить вашу ОС надежными сторожами — программами, которые смогут вовремя распознать и обезвредить прокравшегося в ваше логово врага.

Вопрос лишь в том, какую программу выбрать? Ведь большинство современных антивирусов обещает высокий уровень защиты, все без исключения умеют обновлять свои базы через Интернет... Словом, если судить по рекламе, выбрать можно все, что угодно!

На самом деле это не совсем так. Более того — единой, универсальной программы на все случаи жизни просто не существует!

Еще раз перечислим наших врагов:

- Вирусы.
- «Трояны».
- Руткиты.
- Реклама.
- Шпионские модули.

Прибавьте еще защиту от вторжений, контроль за деятельностью программ, защиту от спама...

Словом — «чудище обло, озорно, стозевно и лаяй». И справиться с этим чудищем в одиночку будет непросто даже самой продвинутой программе. Есть и такие, конечно — мощные и многофункциональные «комбайны» типа **Symantec Internet Security**, **Kaspersky Personal Security** или **Panda Internet Security**. Ах да, не забудем еще и созданный специально для Windows Vista комплекс **Microsoft OneCare**, который только что посуду мыть не умеет.

Теоретически вы можете смело выбирать любую указанную программу, и ее (опять же теоретически) будет достаточно для того, чтобы обезопасить ваш компьютер от большинства угроз. В состав таких наборов входит и антивирус, и сетевой фильтр-файрволл, позволяющий защититься от сетевых вирусов- «червей», «троянских программ» и руткитов. Кроме того, современный антивирус должен уметь обезвреживать «шпионские» программы и рекламные модули — хотя к вирусам они и не относятся, вред от них тоже весьма ощутимый.

Но за все это придется расплачиваться снижением производительности: «комбайны» просто безбожно тормозят систему. К тому же возможности их модулей неравноценны:

- «Касперский» — отличный антивирус, а вот брандмауэр в этом пакете слабоват...

- Продукция Symantec мало того, что отличается чудовищными аппетитами, не слишком удобна в настройке — для новичков это не существенно, но для продвинутых и опытных пользователей порой жизненно важно.
- Что же касается «комбайна» от Microsoft, то его надежность пока что под вопросом, ибо ранее эта компания антивирусами просто не занималась.

Так что, упомянув про комбайны, уделим внимание и отдельным программам, которые порой существенно опережают любые интегрированные продукты.

Антивирусные программы

Антивирус — едва ли не первая программа, которую вам придется установить на свой компьютер сразу после покупки. И уж во всяком случае, не пытаться выходить без него в Интернет!

Но как выбрать? Сегодня антивирусы выпускают все, кому не лень, а коробки с ними продаются чуть ли не в газетных киосках! Существует несколько основных точек зрения на эту проблему.

Ряд пользователей считает, что нет ничего лучше отечественных продуктов, наиболее приспособленных к нашей вирусной «атмосфере». Не стоит сбрасывать со счетов и патриотизм — анекдотично, но даже пользователи пиратских копий отечественных антивирусов свято верят в то, что вносят свой вклад в поддержку российских производителей.

Другие ориентируются на результаты тестов авторитетных западных изданий — и в первую очередь, на хит-парад Virus Bulletin 100 % Awards (http://www.virusbtn.com/100/). Кстати, оба отечественных антивируса неизменно присутствуют в Top10 самых надежных антивирусных программ этого рейтинга, хотя на первых местах неизменно оказываются продукты, о которых наши пользователи и слыхом не слыхивали. А единственная по-настоящему популярная в России западная программа — Symantec Antivirus — неизменно плетется в хвосте списка (что не мешает ей получать множество других авторитетных премий)...

Вот как, например, выглядел рейтинг антивирусов от Virus Bulletin летом 2006 года:

1. Eset (NOD32)
2. Kaspersky Antivirus
3. Dr. Web
3. Norman
4. McAfee Inc
5. VirusBuster

6. Sophos
7. Frisk (F-Prot)
8. Symantec (Norton)

А вот сравнительное тестирование, проведенное в начале 2007 года российским сайтом Anti_Mailware.Ru, демонстрирует совершенно иную картину:

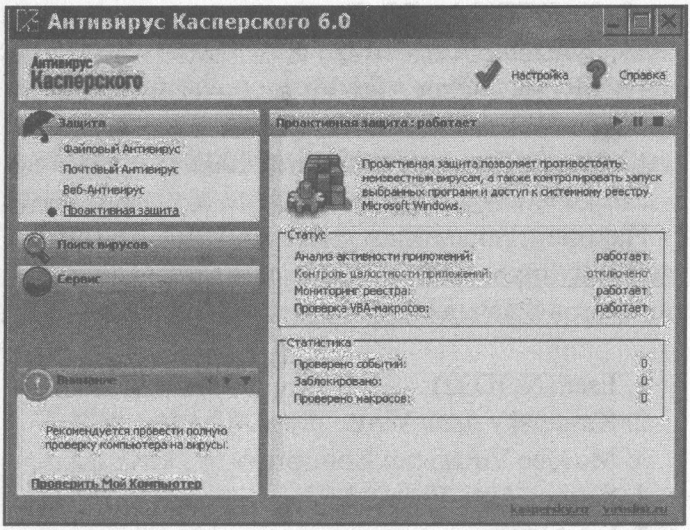
1. Kaspersky 2006
2. F-Secure Anti-Virus 2006
3. CyberScrub AntiVirus
4. eScan Virus Control
5. McAfee VirusScan
6. BitDefender Anti-Virus
7. Eset Nod32
8. H+BEDV AntiVir Personal
9. Symantec Anti-Virus
10. FRISK F-Prot Anti-Virus
11. Dr. Web version
12. Panda Titanium Anti-Virus 2006

Наконец, по данным сайта Antivirus.Ru (http://www.antivirus.ru/OknoA.html) рейтинг лучших антивирусов в начале 2007 года выглядел так:

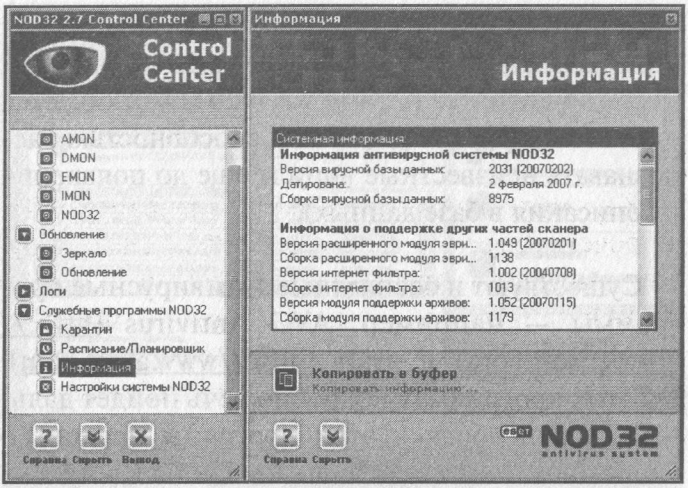
1. Eset (NOD32)
2. Kaspersky Anti-Virus
3. McAfee VirusScan Enterprise
4. Sophos Anti-Virus v.6.03
5. CA eTrust
6. VirusBuster Professional 2006

7. Symantec Antivirus
8. Norman Virus Control
9. Dr. Web
10. Trend Micro OfficeScan Corporate Edition

Какому из рейтингов верить — решайте сами. Впрочем, радует то, что оба российских антивируса — Антивирус Касперского (http://www.kav.ru) и Dr.Web (http://www.drweb.ru) уверенно проходят все без исключения тесты и, стало быть, обеспечивают надлежащий уровень защиты. «Касперский» — рекордсмен по числу отлавливаемых вирусов, к тому же эта программа способна обезвреживать не только классические вирусы и «трояны», но и руткиты, рекламные и шпионские



Антивирус Касперского



NOD32

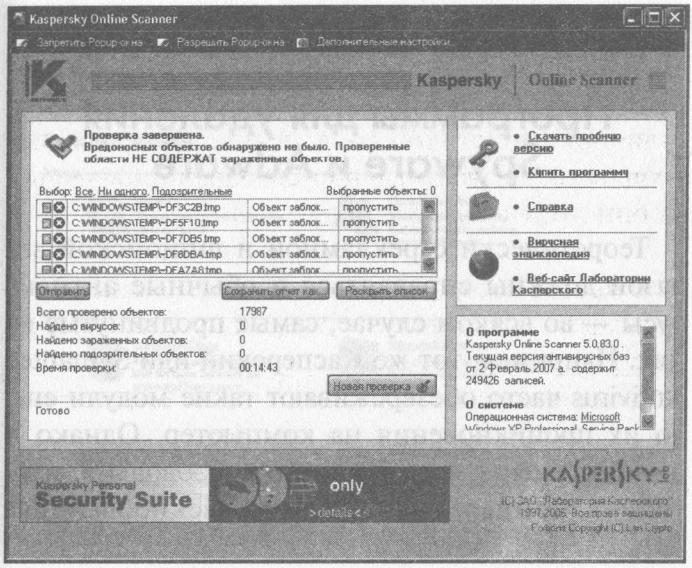
модули. Интерфейс программы прост и понятен даже для новичка, в то же время настройка здесь сделана куда более гибко, чем в «комбайне» от Symantec. Однако назвать «Касперского» идеальным антивирусом для дома мешает его громоздкость и медлительность — KAV очень требователен к аппаратным ресурсам.

Из западных разработок рекомендую обратить внимание на NOD32 (http://www.nod-32.ru). Этот французский антивирус уже давно стал культовым в кругах опытных пользователей — его предпочитают за высокую скорость работы, малый размер и стабильность. Что же касается надежности его работы, то она просто вошла в легенду: NOD более тридцати раз удостаивался высших

наград антивирусного журнала Virus Bulletin, при этом более двадцати раз он оказывался на первом месте в рейтинге! К тому же NOD32 отличается отличной эвристикой (то есть способностью распознавать неизвестные вирусы еще до появления их описания в базе данных).

Существуют и бесплатные антивирусные программы — например, AVG Antivirus (http://www.grisoft.com) и avast (http://www.avast.com). Об этих программах подробно речь пойдет дальше. Возможности у этих программ несколько скромнее: в их составе вы не найдете встроенного фильтра-файрволла, и с рекламным «мусором» (а чаще всего — и руткитами) они бороться не умеют. Однако от действительно опасных вирусов защитят, к тому же эти программы практически не «тормозят» компьютер, чего не скажешь об их «старших братьях». Для слабых офисных машин это порой единственный выбор.

В критических ситуациях, если антивируса под рукой почему-то не оказалось, сойдут и специальные «сканеры» — их также можно скачать абсолютно бесплатно. Если полноценные антивирусы все время «висят» в оперативной памяти и сканируют любой открытый файл или запущенную программу в «теневом» режиме, то сканеры просто проверяют все содержимое жесткого диска. К сожалению, обновлять антивирусную базу таких сканеров в автоматическом



Kaspersky Online Scanner

режиме невозможно — она «зашита» в теле программ, зато новые версии самих сканеров появляются довольно часто. Пожалуй, лучшая программа этого класса — Dr.Web Cure.IT! (http://drweb.ru/download/).

Наконец, проверить свой компьютер можно и вовсе без дополнительных программ — напрямую через Сеть! Многие антивирусные компании в качестве «завлекалочки» размещают на своих сайтах онлайн-сканеры — один из них можно найти на сайте Лаборатории Касперского:

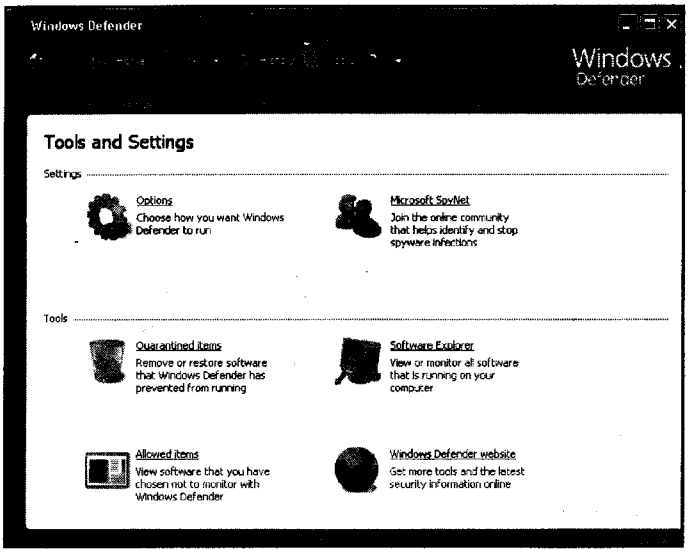
(http://www.kaspersky.ru/virusscanner)

Программы для удаления Spyware и Adware

Теоретически с рекламной и шпионской заразой должны справляться и обычные антивирусы — во всяком случае, самые продвинутые из них. Например, тот же Касперский или Symantec Antivirus часто обезвреживают такие модули еще до их проникновения на компьютер. Однако и они бессильны, если вы сами, добровольно, пустили в компьютер хорошо замаскированного «рекламного агента».

Так что поговорим о том, как максимально быстро и безболезненно вычистить из нашего компьютера всю эту окопавшуюся на нем нечисть.

- Первым делом полностью очистите кеш своего браузера — это можно сделать его собственными средствами: Сервис ▸ Свойства обозревателя ▸ История просмотра ▸ Удалить ▸ Временные файлы Интернета (для Internet Explorer).
- Также это можно сделать с помощью специальных программ-чистильщиков (CCleaner, WinTools.Net, TuneUp Utilities и многих других бесплатных и платных программ).



Windows Defender

- После этого скачайте и установите на компьютер специальную программу для «отлова» adware и spyware. А лучше — даже несколько. Начать можно с бесплатной программы Windows Defender: пользователи Windows XP могут найти ее на сайте Microsoft по адресу:

http://www.microsoft.com/athome/security/spyware/software/

Если на вашем компьютере установлена Windows Vista — Defender уже включен в эту версию.

Руководство Microsoft утверждает, что Defender способен обезвредить до 90 процентов рекламных и шпионских программ. Возможно, это так и есть... Однако нам желательно подстраховаться и взять всемогущему «Дефендеру» помощника. Например, легендарную программу **Ad-Aware**, созданную компанией Lavasoft (www.lavasoft.de).

Ad-aware

(http://www.lavasoft.de)

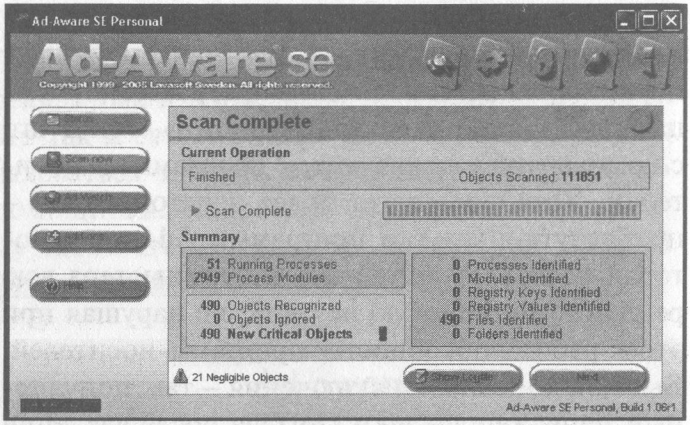
Существует категория «троянских» программ, которые проживают на нашем компьютере вполне легально. Их взяли в союзники производители программного обеспечения, «поселив» их в своих программах категории adware или freeware. Правда, теперь прирученные «троянцы» уже не воруют пароли, а просто работают «подсадными утками», исправно оповещая производителей программ о ваших действиях: куда вы ходите, что ищете, какие сайты предпочитаете. А те в ответ радуют вас хорошей порцией рекламы...

Стоит ли бороться с этими «шпионами»? Пользователи с обостренной совестью считают, что нет у нас на то морального права – за все ведь надо платить. В том числе и за услуги «бесплатных» программ. А потому со вздохом позволяют «троянцам» стучать на себя и добросовестно созерцают всю поступающую рекламу.

Пользователи же с обостренным инстинктом самосохранения не столь покладисты, и при первых признаках наличия в программе «троянца», пусть даже и «окультуренного», гонят его с компьютера в шею вместе с программой-носителем. Хотя существует более простой выход – прибегнуть к услугам программы Ad-aware, которая позволяет вычистить из компьютера всю рекламно-шпионскую нечисть, не нарушая при этом работоспособности программ-носителей. Бывают, конечно, и исключения – так, популярный менеджер докачки Go!Zilla после удаления «троянской» начинки работать отказывается, а вот его коллеги GetRight и FlashGet более покладисты.

Ad-aware выпускается в виде трех версий.

- Базовая, бесплатная, способна только избавить ваш компьютер от уже установленных «шпионских» и рекламных модулей. Работает эта версия как обычный антивирус в режиме «сканера» — на проверку среднего жесткого диска уходит от 3 до 10 минут.
- Платная версия Plus обладает еще и функцией мониторинга — то есть, она способна не просто почистить систему от уже проникшей нечисти, но и предотвратить саму установку шпионских модулей на ваш компьютер.



Ad-Aware

- Наконец, самая мощная версия Professional способна охранять не только один компьютер, а и сразу несколько объединенных в локальную сеть машин.

Все три версии работают с единой базой данных, которую время от времени необходимо обновлять через Интернет. Новые базы для Ad-aware появляются примерно два раза в месяц — этого хватает, чтобы зафиксировать все новые изобретения неутомимых рекламщиков.

Увы, хотя Ad-Aware и стала своего рода символом всех антишпионских программ, результаты тестов показывают, что сегодня ее способности значительно уступают другим, более продвинутым программам. Особенно это касается

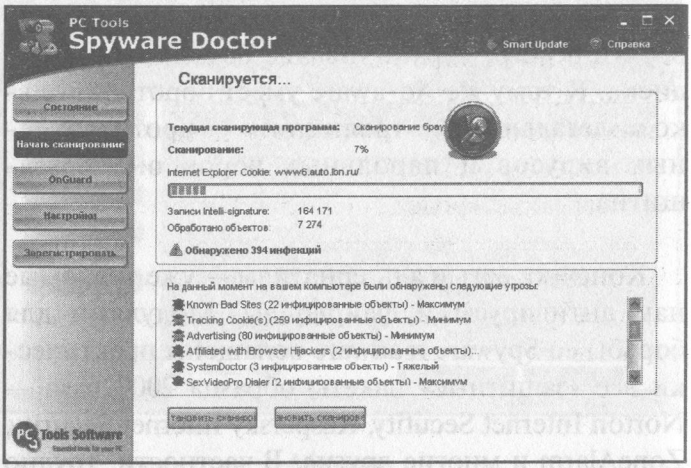
бесплатной версии, которая не умеет даже проверять реестр, ограничиваясь беглым анализом диска. К тому же Ad-aware умеет бороться только с «легальными» «троянцами» — против обычных вирусов и парольных воров она беззащитна.

Конечно, есть и альтернативы — уже знакомые нам антивирусы и файрволлы. Модулями для борьбы со Spyware и adware оснащены практически все «защитные» пакеты образца 2007 года — Norton Internet Secutity, Kaspersky Internet Security, ZoneAlarm и многие другие. В частности, трудно не отметить способности детища Лаборатории Касперского — хотя KIS все же не дотягивает до звания лучшего борца с рекламно-шпионским мусором. Лучшим же выбором остаются отдельные программы — такие как SpySwipper или Spyware Doctor.

Spyware Doctor

(http://www.pctools.com)

Spyware Doctor – одна из самых удобных и наглядных программ этого класса, ее интерефейс уже при установке автоматически настраивается на русский язык, а работа с ней не создает никаких сложностей. Как и большинство других программ, Spyware Doctor состоит из нескольких модулей – резидентного «сторожа», которые предотвращает проникновение на ваш компьютер вредоносной



Spyware Doctor

«начинки» с интернетовских сайтов, сканнера, благодаря которому можно вычистить с диска уже просочившуюся заразу, и почтового модуля.

Программа успешно справляется со всеми категориями adware и spyware, включая «звонилки», «кейлоггеры», троянские и следящие программы.

К примеру, после проверки моего компьютера (до этого просканированного с помощью Windows Defender, Ad-Aware и антивируса NOD 32), на нем было обнаружено более 900 «потенциально опасных» файлов!

В обморок падать не стоит: под подозрение попали и невинные файлы-cookie с различных сай-

тов, а к числу «особо опасных ресурсов» был отнесен даже поисковой портал Яндекс! Однако примерно в двух десятках случаев речь действительно шла если не об особо опасных, то наверняка о «нежелательных» гостях. При заходе на действительно опасные сайты вроде Crack.Am и Интернет-казино Spyware Doctor своевременно оповестил о попытках установки на компьютер скрытых программ.

По результатам тестов эта программа неизменно оказывается в первой тройке «сторожей» (хотя и не всегда занимает первое место). Однако наличие русскоязычного интерфейса – безусловный плюс в глазах российских пользователей, искупающий практически все недостатки программы... Кроме разве что цены.

Межсетевые экраны (файрволлы)

Вы когда-нибудь задумывались над тем, каким именно образом программы (вредоносные или нет — пока не важно) получают доступ к вашему компьютеру через Сеть? Каким именно образом вообще организован обмен данных между вашей «персоналкой» и Интернетом? Как именно компьютер определяет, какую программу допустить к своему мягкому и уязвимому брюшку, а перед какой надобно закрыть все ворота на засов?

Давайте разберемся...

Представим ваш компьютер в виде средневекового замка, окруженного высокой стеной. Пока к замку дорожку не протоптали — жил он вполне самодостаточным образом. Но эволюция на месте не стоит, цивилизация развивается, время налаживать товарообмен с соседями — поэтому в стене прорубается дверь и прокладывается шоссе до ближайшего города. А на ворота ставится стража — чтобы вместе с честными торговцами не проскочила в замок всякая шушера сомнительного происхождения и не менее сомнительной морали...

На этом сходство компьютера с замком заканчивается. Ибо ворота у замка одни, а функцию фильтрующего элемента выполняют сторожевые дуболомы с берданками.

Компьютер же поступает иначе — в своей «защитной стене» он прорубает не одни ворота, а множество. При этом каждый вход он закрепляет за определенной программой или сервисом, который будет отныне полновластным хозяином данной «двери».

Проблема в том, что дверей таких слишком уж много. Протокол TCP, который и является основным для современной Сети, предполагает использование целых 65536 (2^{16}) портов. А ведь могут использоваться еще и другие протоколы — например, UDP, в ассортименте которого находится точно такое же количество портов...

Первые 100 портов (0–99) относятся к категории стандартных — их использование жестко регламентировано и навсегда закреплено за определенными службами. Следующий диапазон портов (до 1024) именуется «широко используемым» и предоставляет своим клиентам чуть меньше полномочий. А вот дальше начинается «темный лес» — более 60 000 портов, большая часть которых дается на откуп сторонним программам.

В идеале открытыми для использования могут быть лишь те порты, которые зарезервированы за определенными, известными системе программами — остальные «двери» должны быть надежно заблокированы. К тому же для каждого порта должны быть созданы четкие правила, каждому должны быть делегированы свои полномочия. Одни из них открыты только на «вход», другие — на «выход» информации, а третьи допускают и двустороннюю передачу данных. Ведь мы же не только скачиваем информацию из Сети — порой нам приходится и отправлять туда информацию в виде команд или данных...

Но самое главное — не должно случаться так, чтобы, получив доступ к компьютеру через какой-либо порт, программа (или управляющий ею человек) могли пуститься во все тяжкие — копировать или изменять файлы на компьютере, вносить изменения в настройки системы.

В теории так и предусмотрено. Однако на деле в системе защиты Windows имеется множество «дырок», которые позволяют злоумышленнику получить доступ к вашей информации через «недозволенный» канал. Конечно, это не значит, что, получив доступ к определенному порту, вы можете хозяйничать в чужом компьютере, как в собственной «персоналке» — такое бывает только в кино. К тому же просто так, наобум, ломиться в любой попавшийся логический порт бесполезно — атаки на большинство из них успешно отражаются самой операционной системой.

Но иногда достаточно лишь крошечной ошибки, позволяющей человеку, оседлавшему определенный порт, получить немного больше простора для маневра, чем было задумано изначально.

Возьмите, к примеру, вирус Blaster, который атакует компьютер через порт 135 или 139. Этот порт относится к числу «широко используемых» — а значит, операционная система теоретически должна за этим портом пристально следить, не позволяя использовать его для нежелательных операций. Однако благодаря крохотной «дырочке» в системе защиты вирус получает возможность выполнить действие, приводящее к перезагрузке компьютера, которое повторяется вновь и вновь при каждом входе в сеть. Это, конечно, не форматирование диска... Но и перезагрузка компьютера в разгар работы — не самое приятное в жизни событие...

А ведь портов в компьютере десятки тысяч, и пресловутая «дырка» — далеко не единственная брешь в защите Windows...

➔ Кандидат на «взлом» может быть выбран как случайно, так и намеренно — достаточно лишь отследить момент, когда нужный вам пользователь войдет в сеть. Конечно, при модемном соединении, когда времени на сканирование у вашего противника немного, вероятность «взлома» не так уж высока. Но при постоянном подключении к сети (например, кабельном) опасность «взлома» резко возрастает.

Существуют специальные программы для сканирования портов, с помощью которых можно отыскать лазейку практически в любой компьютер. Или наоборот — выход из него. Именно так работают многие «троянские» программы, отправляющие данные из вашего компьютера.

Защититься от подобных атак традиционными способами уже не получится. Антивирус бессилен — это не по его специальности, да и встроенная защита Windows частенько пасует... Однако рецепт спасительного «лекарства» от этой болезни все же существует. Состоит он из двух частей:

⏭ Регулярно скачивать обновления для вашей версии Windows. Напомним, что для этого

достаточно просто зайти на сайт Центра обновления Windows (http://windowsupdate.microsoft.com) или щелкнуть по значку Центр обновления Windows в меню Сервис программы Internet Explorer.

⏭ Установить специальную программу, которая возьмет на себя полный контроль над всеми портами и сможет оперативно оповестить вас об атаке. А то и просто отразить ее. Такие программы называются файрволлами (firewall) или брандмауэрами. В переводе на русский эти слова означают — «огненная стена». Смысл названия двоякий — во-первых, преодолеть сплошную стену огня невозможно, если только ты не пожарный-профессионал. А с другой стороны, название это напоминает о хорошо известном способе тушения лесных и степных пожаров: навстречу надвигающейся огненной лавине пожарные пускают вторую, специально поджигая лес. Две огненные стены встречаются — и в мгновение ока уничтожают друг друга.

Точно так же работают и компьютерные файрволлы, защищая наш компьютер от проникновения заразы извне. Непреодолимой стеной встают они на пути разрушающих программ и скриптов, а атаке через порты противостоят, пользуясь оружием самих нападающих — сканируя порты доступа.

Обнаружив попытку несанкционированного проникновения в ваш компьютер, программа может просто подать сигнал тревоги, а может сразу заблокировать доступ подкапывающемуся под вас «кроту». Это — основная функция всех программ этого класса, к которой, в зависимости от сложности продукта, добавлено еще множество других, более или менее нужных.

...Увы, приходится огорчить всех тех, кто считает персональные файрволлы надежной защитой. Практика показывает, что большинство из этих программ-«стражей» довольно уязвимы, они могут отбить атаки лишь не слишком умелых хакеров. Против настоящих профессионалов взлома они, увы, бессильны. Если же вы хотите проверить, насколько «дыряв» ваш любимый файрволл, воспользуйтесь услугами утилит **Firewall Leakage Tester** и **Firehole**, которые вы сможете найти на большинстве сайтов по компьютерной безопасности.

Существует и масса специализированных сайтов, которые позволят вам проверить защищенность вашего компьютера через Интернет. Например, такую услугу предлагает один из разделов корпоративного сайта Symantec (http://www.symantec.com/sabu/nis/nis_pe/).

Кроме того, проверить свой файрволл на уязвимость можно по одной из этих ссылок:

http://scan.sygate.com
http://www.auditmypc.com
http://www.pcflank.com/test.htm
http://www.hackerwatch.org/probe/

Прибегать к услугам брандмауэров приходится даже пользователям Windows XP — притом, что в новых операционных системах Microsoft уже имеется встроенный брандмауэр. Однако удобство работы с ним оставляет желать лучшего, хотя надежность встроенного «сторожа» порой даже выше, чем у отдельных программ этого типа.

Основных требований к современному файрволлу несколько:

- Он должен уметь отражать атаки не только извне (попытки сканирования портов), но и изнутри.
- Файрволл должен отслеживать активность установленных в вашей системе программ и позволять вам блокировать доступ к Сети любой из них.
- Наконец, файрволл должен предоставлять вам возможность выборочного закрытия отдельных портов (причем с учетом направления — «вход» или «выход», а также — конкретного протокола).

Пользователям домашних компьютеров, подключенных к скоростному выделенному каналу, рекомендуется вручную закрыть доступ к следующим входящим портам (с указанием протоколов доступа).

TCP:20,
TCP:25,
TCP:69,
UDP:69,
TCP:135,
UDP:135,
UDP:137,
TCP:139,
UDP:139,
TCP:445,
UDP:445,
TCP:555,
TCP:4444,
TCP:12345,
TCP:54321,
TCP:54320,
TCP:65000

➔ Конечно, на самом деле «опасных» портов куда больше. Но это — тот необходимый минимум, который может уберечь вас от множества неприятностей. Специалисты по компьютерной безопасности и «продвинутые» пользователи могут заглянуть, к примеру, на сайт компании Commodon, где опубликован впечатляющий список потенциально опасных портов с указанием программ, которые их используют:

http://www.commodon.com/threat/threat-allports.htm

Большинство современных «сторожей», помимо своей прямой обязанности, умеют выполнять и ряд других полезных функций — напри-

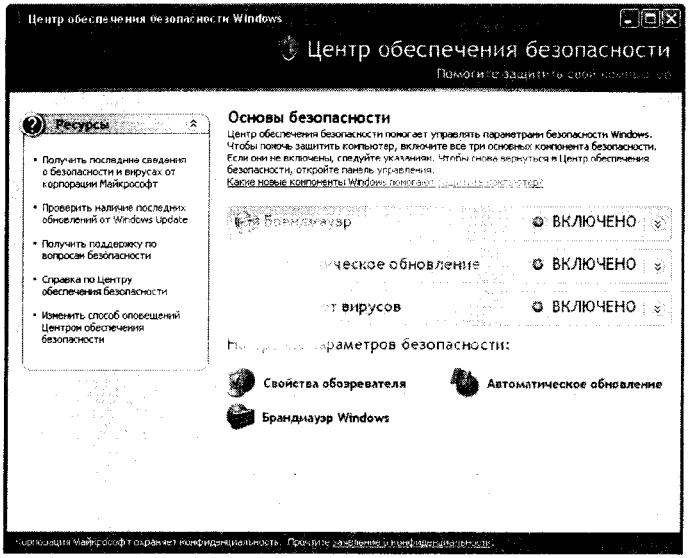
мер, удалять с сайтов надоедливые рекламные баннеры, предотвращать роение выпадающих окон с той же рекламой. Словом — выступают еще и в качестве оптимизаторов и ускорителей. Вот почему автор позволит себе не согласиться с теми, кто утверждает, что в этих программах (в связи с их ненадежностью) и вовсе нет никакой необходимости.

Центр безопасности Windows

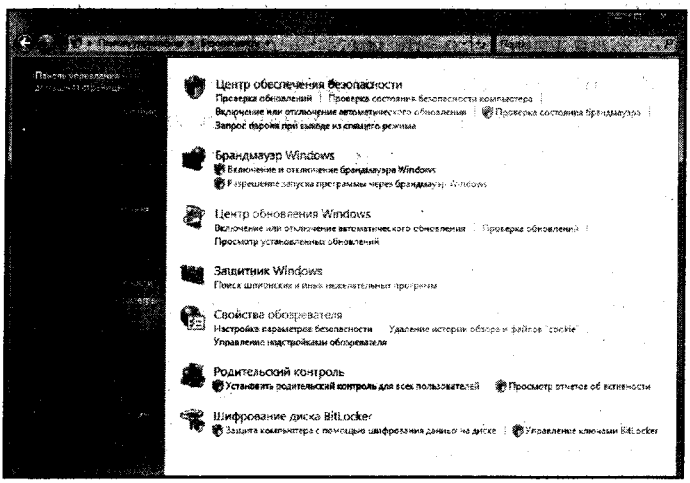
Начать знакомство с файрволлами можно со встроенного «сторожа», включенного в Windows XP. Хотя удобство работы с ним оставляет желать лучшего, однако надежность встроенного файрволла порой даже выше, чем у отдельных программ этого типа. Найти его можно в разделе ***Центр обеспечения безопасности*** Панели управления Windows XP. Если же такого значка нет, вероятнее всего, у вас установлена устаревшая версия XP — брандмауэр появился лишь в пакете обновлений Service Pack 2.

Для настройки файрволла зайдите в раздел ***Настройка параметров безопасности*** и выберите значок ***Брандмауэр Windows***.

Если на вашем компьютере не установлен другой, более совершенный «сторож», рекомендуется сразу же включить стандартный брандмауэр (вкладка ***Общие***). В противном случае его лучше



Центр обеспечения безопасности



Центр обеспечения безопасности Windows Vista

выключить, невзирая на панические предупреждения системы безопасности. Совместная работа сразу двух файрволлов вряд ли улучшит «броню» вашего компьютера... А вот стабильность работы снизит точно.

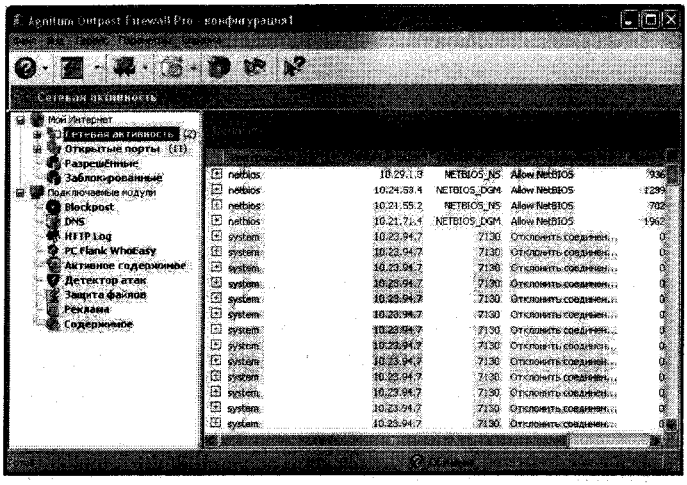
Как любой стандартный продукт от Microsoft, файрволл Windows XP не рассчитан на тонкую подстройку — теоретически он сам должен определять все возможные виды атак и блокировать опасные программы. Однако во вкладке ***Исключения*** вы можете указать программы, которым этот суровый сторож даст «зеленый свет». Здесь же опытные пользователи могут вручную открыть тот или иной нужный порт. И все же этого мало, крайне мало...

Даже в том случае, если вы и вынуждены на какое-то время довериться «штатному» файрволлу, постарайтесь побыстрее заменить его на более удобную и функциональную программу — благо их сегодня на рынке вполне достаточно.

Outpost Firewall

(http://www.outpostfirewall.com)

Эта программа отечественного происхождения отличается предельным аскетизмом интерфейса и максимальной гибкостью настроек. И не только



Outpost Firewall

допускает, но и предполагает самостоятельную настройку. При грамотном подходе эта программа превращается в один из самых мощных и надежных файрволлов, обладающих, к тому же, массой интересных изюминок.

Помимо своих прямых обязанностей (фильтрация входящего и исходящего трафика, контроль за запущенными программами) Outpost способен блокировать рекламные вставки на вебстраницах, а в случае необходимости — и ограничивать доступ к «опасным» сайтам. Интересно, что Outpost, в отличие от большинства своих коллег, может обучаться новым трюкам с помощью дополнительных модулей-плагинов. В том числе и созданных сторонними разработчиками. Около

десятка самых удачных плагинов встроено в Outpost Pro изначально, другие можно скачать и установить дополнительно.

Вот лишь некоторые из возможностей Outpost, которыми программа обязана именно предустановленным плагинам.

Детектор атак. Ловит и блокирует все известные Интернет-атаки. Замечает любой вид сканирования портов. Распознает и блокирует сложные DoS атаки. Может быть настроен блокировать IP адрес и подсеть атакующего.

Блокировка содержимого. Может блокировать целые домены, такие как sex.com, или любые другие страницы, содержащие специфические слова «бомба», «взрывчатка в домашних условиях», «секс» и др. Однажды настроенный модуль, который нельзя изменить без пароля, делает его идеальным для родителей и работодателей.

Кеширование DNS. Кеширует все разрешенные DNS имена в специальной базе, что значительно уменьшает время соединения (при посещении сайтов, получении/отправке почты, новостей, сообщений ICQ и т. д.).

Фильтрация активного содержимого. Блокирует cookies, историю посещений сайтов,

Java апплеты, Java скрипты, VB скрипты в веб-страницах, почте и новостях. Для каждого сайта можно разрешить или запретить то или иное активное содержимое.

Защита почтовых вложений. Блокирует «трояны», вирусы, червей, VB вирусы (как Melissa) во вложениях входящей почты. Блокировка активных элементов в e-mail.

Из дополнительных плагинов самым интересным является WhoEasy, который позволяет вам узнать максимум сведений об атаковавшем вас человеке по его IP-адресу (адрес и имя провайдера, телефонный номер администратора сети).

Радует интерфейс программы — компактный, удобный и открытый: вам не придется рыскать в его дебрях. Однако не наблюдается здесь и «синдрома ZoneAlarm»: простота простотой, но возможность тонкой подстройки любого из инструментов Outpost также присутствует. Например, создать правила для блокировки портов здесь так же легко, как и правила для сортировки почты в знакомом всем нам Outlook Express. Сделать это можно в меню ***Параметры*** ▸ ***Системные*** ▸ ***Общие правила***.

Работа с правилами в Outpost реализована очень интересно: правила позволяют программе

не только блокировать порты, но и совершать любые другие действия. Так, например, при обращении к определенному сайту или порту программа может выключить компьютер (подобные штучки обычно приходятся по вкусу родителям, стремящимся контролировать сетевые путешествия чада), запустить другую программу или вывести текстовое сообщение. Разумеется, для каждой программы можно создавать сложные правила, которые регламентируют доступ к портам, сетевым ресурсам и т. д.

Как и в случае с другими файрволлами, оптимальным режимом работы Outpost является «**обучающий**» — программа будет регулярно спрашивать вас, разрешить или нет доступ к Сети тому или иному приложению. При однозначном ответе «Да» в дальнейшем Outpost не будет мучить вас вопросами, однако можно разрешить лишь однократный допуск приложения к заветному каналу, оставив окончательное решение ее судьбы на потом.

Помимо обучающего режима, существует еще три:

- Режим разрешения (соединяться с Интернетом разрешено любым программам, за исключением внесенных в «черный список»).

- Режим запрещения (блокируется доступ к Сети любых программ, за исключением внесенных в «белый список»).
- Режим бездействия (приостановка работы файрволла).

После установки программа автоматически создает правила доступа для большинства популярных программ — в Outpost уже имеется большая библиотека «шаблонов». Так что в большинстве случаев вам даже не придется мучительно думать, пускать в Сеть тот или иной модуль или нет.

Кроме платной версии Pro существует еще и бесплатная модификация Outpost, лишенная ряда важных, но не принципиальных, возможностей — например, она не умеет блокировать рекламу, создавать «расширенные» правила и т. д.

Еще одна интересная особенность Outpost — открытая архитектура: программу можно снабдить новыми интересными функциями за счет подключения внешних модулей, написанных независимыми программистами.

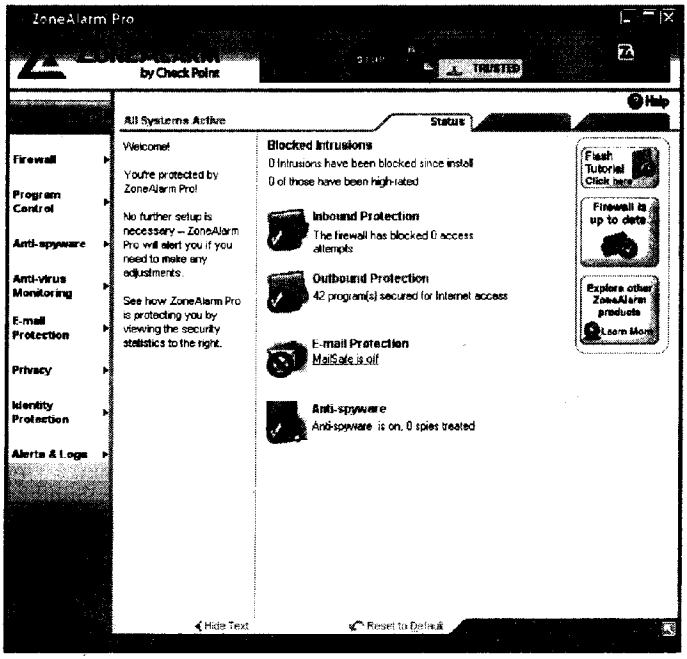
Кстати, и обновляется Outpost куда чаще других файрволлов — новая версия программы выкладывается на страничке практически еженедельно.

ZoneAlarm

(http://www.zonelabs.com)

Один из самых известных и популярных брандмауэров. Простота, простота и еще раз простота — вот девиз создателей этого продукта.

При работе с базовой, бесплатной версией программы от вас требуется всего лишь отрегулировать требуемый уровень безопасности — **«слабый»**, **«обычный»** или **«высший»**. После этой безумно сложной процедуры программа мирно



ZoneAlarm

свернется в значок в правом нижнем углу экрана, давая о себе знать лишь в тот момент, когда какая-то программа затребует разрешить ей доступ в сеть.

Если это будет, к примеру, браузер или клиент электронной почты — все в порядке: смело давайте ZoneAlarm команду на разрешение доступа, и в дальнейшем она уже не будет вас беспокоить по столь пустяковому поводу. Но если вы видите, что в сеть рвется совершенно посторонняя программа... что ж, возможно, имеет смысл воздвигнуть на ее пути заслон.

Кстати, при помощи ZoneAlarm можно не просто «окоротить» отдельную программу, но и мгновенно «заморозить» весь поток данных, льющийся от вашего компьютера в сеть и обратно. Эта возможность — уникальная, практически у всех коллег ZoneAlarm она отсутствует.

Для тех программ, которым по своей природе можно и даже нужно регулярно лазить в сеть, ZoneAlarm использует уникальный, присущий только ему механизм шифрованной подписи, что позволяет выявить маскирующихся под полезные программы «троянцев». Этим во многом и объясняется высокая эффективность ZoneAlarm при борьбе с этим классом заразы. Заодно она надежно защитит вас от попыток «нюкнуть» ваш компьютер или просканировать порты.

Но простота и бесплатность, простите за каламбур, не дается даром: ZoneAlarm вряд ли справится с вирусной атакой (хотя блокировать «троянцев» и некоторых «червей» она сможет) или «скриптами-убийцами». Поэтому, познакомившись на его примере с алгоритмом работы файрволлов, стоит поискать продукт классом повыше. Часть этих функций (например, антивирусная защита, а также механизм защиты и шифрования системных паролей) реализована в профессиональной, платной версии программы — ZoneAlarm Plus. Версия же Pro заодно умеет бороться и с рекламными модулями на страничках — всплывающими окнами, баннерами и т. д.

В самую продвинутую версию — ZoneAlarm Security Suite — встроен антивирус (на базе C.A Vet Anti-Virus), а также модули для обеспечения приватности и фильтрации веб-контента.

Как в любом серьезном файрволле, в платной версии ZoneAlarm Pro вы сможете самостоятельно задать список блокируемых портов — пусть и не так просто и удобно, как в Symantec Internet Security. Зато работает программа гораздо быстрее.

КОНФИДЕНЦИАЛЬНОСТЬ И ПРИВАТНОСТЬ В WWW

Атаки, мелкие и крупные пакости в ваш адрес — все это раздражает и портит настроение. Но порой куда чаще выводит из себя... обычное наблюдение за твоими действиями. Неустанное и неусыпное. Не прерывающееся ни на секунду...

Ученые говорят, что отсутствие хоть толики уединения, приватности способно свести человека с ума в самые короткие сроки. Вспомним страдания героя Джима Керри в фильме «Шоу Трумена» — а ведь с парнем-то и не делали ничего страшного, не пытали и «Маски-шоу» на дому не устраивали. Просто — наблюдали...

Не будем сгущать краски. С ума никто нас, конечно, сводить не собирается... Но время от времени возникает в сознании навязчивый вопрос: «А не контролируют ли мои путешествия по Се-

ти?». Неважно кто — начальство, коллеги по работе или любимые всеми фибрами души домашние. Неважно, по какой причине — начальству или службе безопасности на работе это по должности положено, и в большинстве западных компаний такая слежка в порядке вещей. Неважно и то, что ничего противозаконного вы не делаете — по неприличным сайтам не шатаетесь, наркотиками в Сети не торгуете...

Словом, несмотря ни на что любой человек хочет обеспечить себе «зону интимности» — и это его законное право. Тем более, что сделать это не так уж и трудно.

Прокси-серверы

У проблемы конфиденциальности во Всемирной Паутине существует и еще одна сторона. Допустим, вам совершенно безразлично, следят или нет за вашими перемещениями домашние, но в то же время вам страшно не хочется, чтобы вас «посчитал» какой-либо из посещенных вами серверов. Мало ли что... Известно ведь, что любой зашедший на страничку пользователь неизбежно оставляет «следы»: IP-адрес его компьютера фиксируется в журнале-«логе» сервера.

А ведь IP-адрес может привести любого желающего прямехонько к вашему реальному, домашнему адресу или телефону...

И дело не только в этом. Честному пользователю бояться этого нет резона — фиксируйте на здоровье! Однако существуют сайты, маскировочным способностям которых позавидуют и хамелеоны: каждому своему гостю они представляют совершенно различную информацию, в зависимости от того, из каких краев тот пожаловал. Частенько этот сервис удобен, но иногда серьезно раздражает. Другие сайты и вовсе не настроены раскрывать свою душу перед посторонними — американцев, к примеру, ждут с распростертыми объятиями, а перед жителями других стран опускают виртуальный шлагбаум. В лучшем случае — интеллигентно выталкивают в шею на свое региональное отделение.

Для преодоления этой напасти можно прибегнуть к услугам «веб-маскировщиков» (anonymizer) или столь же анонимных прокси-серверов.

С прокси-серверами мы уже свели беглое знакомство в разделе, посвященном настройке Интернета. И помним, что так именуется компьютер (или — специальная программа), через который и происходит наше с вами общение с Сетью — именно через него отправляются все наши запросы на получение информации со страничек или файлов. Прокси не просто служит «воротами» в

Интернет и «копилкой» для проходящей через него информации: он может защищать ваш компьютер от вредоносных программ или не слишком желательной (с точки зрения провайдера) информации.

Полный адрес прокси-сервера состоит из его имени и порта доступа, например:

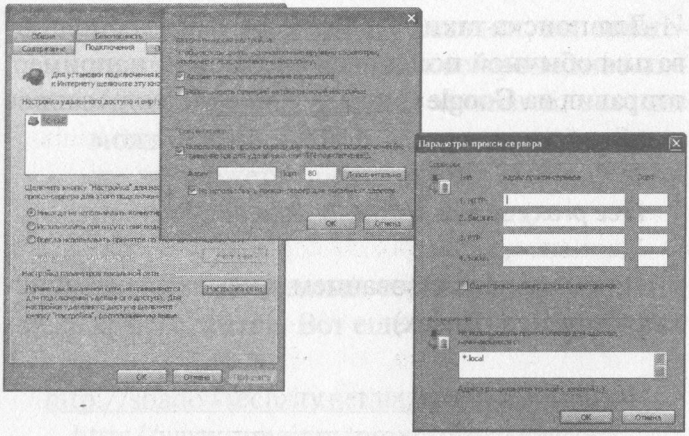
Имя	**Порт**
proxy.provider.net	8028

Кроме того, стоит выяснить, какие именно протоколы может обслуживать ваш прокси — одни специализируются только на WWW-запросах, другие поддерживают еще и FTP.

Все реквизиты прокси-сервера вводятся, как мы помним, в меню ***Сервис*** ▸ ***Свойства обозревателя*** ▸ ***Подключение*** ▸ ***Настройка*** Internet Explorer.

Как правило, адрес прокси-сервера из собственных запасов предоставляет вам провайдер. Однако в некоторых случаях бывает полезно заменить ваш стандартный прокси-сервер на другой — анонимный. И главное — общедоступный.

Дело в том, что стандартные прокси-серверы обладают, к великому сожалению пользователей, некоторыми задатками порядочности — обращаясь по просьбе пользователя к удаленному ком-



Настройка прокси-сервера в Internet Explorer

пьютеру, они сообщают последнему не только свой собственный сетевой адрес, но и IP-адрес пользователя-«заказчика». Разумеется, последнего в итоге не слишком трудно вычислить...

Не надо думать, что теперь хозяин любого посещенного вами сервера может узнать ваше имя, домашний адрес, а заодно и номер счета в банке — такие детали интересуют не слишком многих. Однако и информацию более общего плана (из какой страны «пришел» пользователь, через какого провайдера подключился) в некоторых случаях уместно скрыть, если уж вы так озабочены проблемами анонимности. В этом вам и помогут «анонимные» прокси, которые свой адрес сообщают с удовольствием, а ваш, пользовательский — нет.

Для поиска таких серверов разумно воспользоваться обычной поисковой службой — например, отправив на **Google** (http://www.google.com) запрос типа:

Free proxy server

Или же с использованием русских служб поиска (например, **Яndex**):

Анонимный proxy

Обновленные списки бесплатных прокси-серверов вы всегда можете найти на одной из следующих страничек:

http://free-proxy.da.ru
http://www.proxychecker.ru
http://tools.rosinstrument.com/proxy/
http://www.atomintersoft.com/products/alive-proxy/proxy-list/
http://www.geocities.com/SiliconValley/Network/1120/proxy.html
http://lightning.prohosting.com/~proxy7/index.html

Особенно рекомендую вам первый сайт в этом списке — здесь, помимо собственно списка бесплатных прокси, вы найдете все необходимые программы для работы с ними и массу интересных статей по вопросам компьютерной безопасности. А нажав

кнопку **О вас** внизу странички, вы сможете лично убедиться, какое громадное количество информации о вашей системе можно извлечь при заходе на сайт. Здесь же вы можете проверить выбранный вами прокси-сервер на анонимность.

Кстати, этот полезный сервис представляет и масса других сайтов. Вот еще несколько адресов:

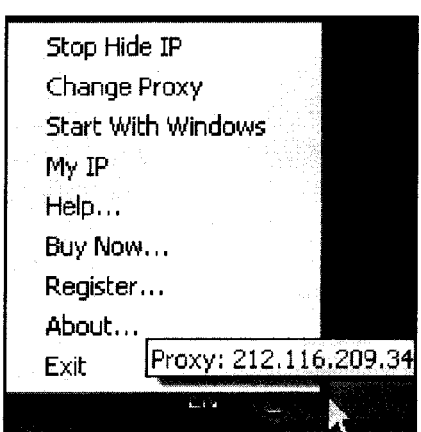
http://shadowsecurity.net.ua/r/checking2.shtml
http://www.samair.ru/proxy/proxychecker/

Самые ретивые сторонники анонимного серфинга порой не ограничиваются одним-единственным прокси, а задействуют целую цепочку серверов! Вот тут уж не подкопаешься — если работа через один-единственный «анонимный прокси» по-настоящему анонимной не является (ваш IP-адрес остается в «логах» сервера, откуда его при желании очень легко добыть), то цепочка из двух-трех серверов поставит надежную преграду на пути желающих сунуть свой любопытный нос в ваши дела...

Правда, стандартные программы для путешествия по Сети такую цепочку организовать не позволяют — ну да не беда, у нас под рукой всегда имеется множество отдельных утилит. Например, **Anonymity 4 Proxy** (http://www.inetprivacy.com), **Multiproxy** (http://www.multiproxy.org) или **SockChain** (http://www.ufasoft.com/socks/).

Кстати, разработчик первой утилиты, компания iNetPrivacy, предлагает еще одну очень полезную программу **AntiFirewall** — она позволяет вам использовать стандартные сервисы Сети (ICQ, электронная почта, IRC, FTP) даже в том случае, если доступ к ним блокирован брандмауэром. Эта крохотная утилитка прямо-таки осчастливила моих знакомых, которые до той поры были лишены радости общения с любимой «аськой» со своего офисного компьютера — постарался не в меру ретивый администратор...

Однако самой большой популярностью среди любителей «приватного серфинга» пользуется утилита **Hide IP Platinum** (http://www.hide-ip-soft.com).



Hide Ip Platinum

Эта программа умеет работать в связке с любым браузером — от последних версий Internet Explorer до Firefox и Opera. Hide IP позволит вам заменить при серфинге ваш настоящий IP на посторонний адрес, который может быть «приписан» не только к другой стране, но и к другому континенту! В сокрытии вашего «истинного лица» участвуют десятки анонимных прокси-серверов, разбросанных по всему миру: программа автоматически выберет среди них самый быстрый и периодически будет переключаться от сервера к серверу, не требуя от вас никаких дополнительных телодвижений. Кроме того, программа может выступить в роли чистильщика, удалив с жесткого диска следы ваших путешествий.

Одной из самых модных новинок этого сезона стал специальный браузер для безопасного серфинга **Torpark** (http://www.torrify.com), созданный группой энтузиастов на основе популярного браузера Firefox. Torpark специально оптимизирован для работы с флеш-карты или брелка, так что вы можете всегда носить его с собой и запускать, к примеру, в Интернет-кафе. К тому же в программу уже встроены средства для скрытия реального IP-адреса, что позволяет быть уверенным: следов вашего путешествия не остается ни внутри, ни «снаружи» компьютера.

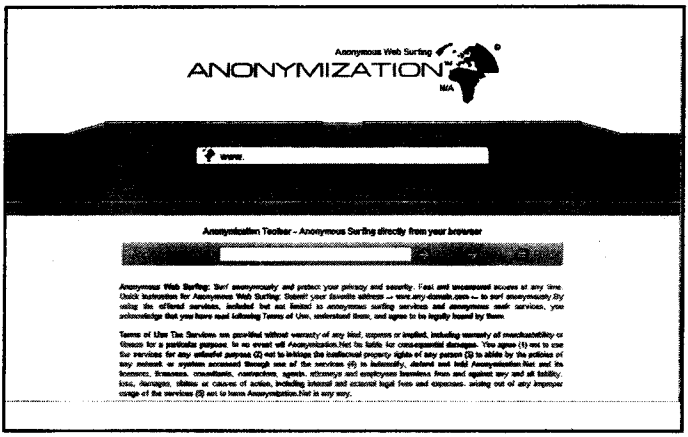
Появление Torpark всерьез озадачило правоохранительные органы разных стран: в некоторых государствах эта программа была внесена в «чер-

ный список», как орудие «педофилов, террористов и наркоторговцев». Искренне надеюсь, что ни один читатель нашей книги ни к какой из упомянутых категорий не относится... Но доля здравого смысла в рассуждениях властей есть: честному человеку скрывать действительно нечего — даже от своих близких.

Веб-маскировщики и «анонимайзеры»

Второй вид «обезличивающих» пользователя служб — «веб-маскировщики», доступ к которым вы можете получить через обычную WWW-страницу. Среди бесплатных служб этого типа можно выделить **Anonymizer** (http://www.anonymizer.com), **Anonymization** (http://www.anonymization.ne/), **ProxyWeb** (http://www.proxyweb.com) и целый ряд других.

Маскировщики работают по тому же принципу, что и прокси-серверы, однако они могут не только обеспечить вам анонимность во время странствий по Сети, но и отчасти защитят вас от вредоносной «начинки» некоторых страниц (всплывающих рекламных окон, «скриптов-убийц» и т. д.).



Anonymization

Для анонимного доступа к любой страничке нужно лишь зайти на сайт-«маскировщик» и набрать нужный URL в его адресной строке. При необходимости страничку «маскировщика» можно сделать «домашней» для вашего браузера, нажав кнопку ***С текущей*** в меню ***Сервис*** ▸ ***Свойства обозревателя*** ▸ ***Общие*** Internet Explorer.

Теперь вместе с вашим браузером будет загружаться и страничка службы анонимного доступа — а значит, пользуясь ее адресной строкой, вы будете защищены от «слежки» во время всего сеанса работы в Сети.

Для пущей же надежности можно объединить способности «маскировщика» и анонимного прокси-сервера — это даст наилучший результат.

Конечно, с точки зрения наших спецслужб столь рьяно ратовать за полную анонимность могут лишь параноики да люди с нечистой совестью... Представьте себе, к примеру, человека, который проходит ежедневный маршрут от дома до метро, нацепив темные очки и петляя по переулкам, дабы сбить с толку мнимых преследователей!

Но есть и другая точка зрения, основанная на гарантируемом Конституцией праве любого человека на неприкосновенность своей частной жизни. К которой, как ни крути, относится и Интернет-серфинг...

Как «замести следы» при работе в Сети

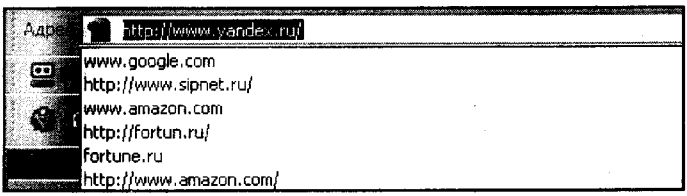
Известно, что ваши путешествия по веб-страничкам могут фиксироваться как самим браузером, так и внешними программами — например, «гейтом» или «файрволлом», через который подключена к Интернету локальная сеть вашего дома или фирмы. С внешними «протоколами» мы ничего поделать не сможем, однако на своем компьютере «спрятать концы в воду вполне реально.

Какие же запрятанные в системе «шпионы» могут рассказать случайному гостю компьютера о наших предпочтениях?

Журнал. Эта папка Internet Explorer не раз выручала нас в те моменты, когда мы не могли вспомнить адрес случайно найденной накануне веб-странички: она всегда готова продемонстрировать нам полный список сайтов, которые мы посетили за последний день, неделю или месяц. Но подобная услужливость может стать и помехой — если свой маршрут можете отследить вы, так же легко это смогут сделать и ваши близкие. И просто любопытствующие. Поэтому время от времени журнал лучше очищать, сохраняя самые интересные сайты в папке закладок.

Закладки. Они тоже могут служить отличной картиной ваших интересов и предпочтений. Но что делать — без закладок мы в любом случае не обойдемся, и чистить их каждый день нам как-то не с руки... Могу предложить самый простой вариант: создайте в Избранном папку под каким-нибудь скучным названием и кидайте все «секретные» закладки именно туда. В конце концов, при сохранении закладок можно давать им не предлагаемые сайтом имена, а свои собственные.

Адресная строка браузера. У нее своя, особая история — и даже после того, как вы очистите «Журнал», все введенные вами в стро-

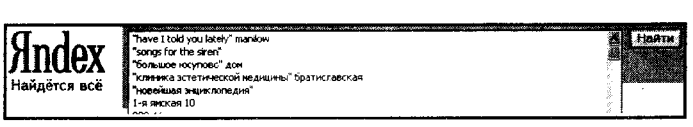


История адресной строки

ке адреса будут высвечиваться, как только вы щелкните по ней мышкой или наберете несколько букв.

История поисковых запросов. Строчки запросов поисковиков Google, Яндекс и других отличаются не меньшей «болтливостью», чем адресная строка вашего браузера. А вдруг среди ваших запросов попадутся такие, которые нежелательно было бы выносить на всеобщее обозрение?

Cookies. Файлы cookies («пирожки») сохраняют на вашем диске многие Интернет-страницы. Сохраняют, в общем-то, с благими целями: благодаря «пирожкам» страничка может «узнать» вас при следующем визите и будет каждый раз вежливо приветствовать вас, называя по имени, а заодно и предлагая вам именно те услу-



История поиска в Яндексе

ги, которые вы затребовали в прошлый раз. «Пирожками» активно пользуются многие сайты: интернет-магазины, поисковики, порталы и блоги... Словом, почти все. Для нашей приватности cookies наименее опасны — простые пользователи вряд ли будут выискивать в них криминал. Разве что зайдут ненароком на какой-то сайт — и с удивлением обнаружат, что вы там уже побывали...

Папка временных файлов Интернета (кеш). Именно здесь покоятся бренные остатки тех страничек, которые вы открывали на вашем компьютере. Разбираться в этом мусоре довольно сложно, однако вполне реально привести эту кучу в удобный для просмотра вид с помощью специальных программ. К тому же кеш-файлы съедают кучу полезного места на жестком диске — хотя лишних 100–200 Мб для нынешних винчестеров мало что значат...

Да уж, наследили мы изрядно, и теперь нам придется изрядно попотеть, чтобы уничтожить все возможные улики. Некоторые параноики делают это едва ли не после каждого сеанса работы — но мы-то с вами ничего криминального не совершали, поэтому чиститься будем только в крайних случаях. Например, когда к вашему компьютеру нагрянет с визитом чрезмерно любопытный отпрыск, младший брат или сестренка.

Для чистки можно использовать встроенные инструменты вашего браузера: их вы можете найти в специальном меню Internet Explorer:

Сервис ▸ Свойства обозревателя ▸ Общие ▸ Очистить охраненные файлы (Internet Explorer 6)

Сервис ▸ Свойства обозревателя ▸ Общие ▸ История просмотра ▸ Удалить (Internet Explorer 7)

Только не делайте полную чистку без нужды: порой достаточно очистить лишь список посещенных вами страниц (***Журнал***), кеш браузера (***Временные файлы Интернета***). Меню ***Данные***

Очистка истории работы в сети в Internet Explorer

веб-форм поможет, в частности, избавиться от истории поисковых запросов в строке Google, Яндекса и других поисковиков. Однако тут надо быть очень осторожным: вместе с водой можно выплеснуть и ребенка! Ведь эта команда очищает абсолютно все данные форм, которые вы когда-либо вводили, а многие из них стоит и сохранить.

Поэтому я рекомендую простой, но действенный способ выборочной очистки: благодаря ему вы можете удалить из строчки поисковика отдельные запросы, которые вы не хотели бы демонстрировать посторонним.

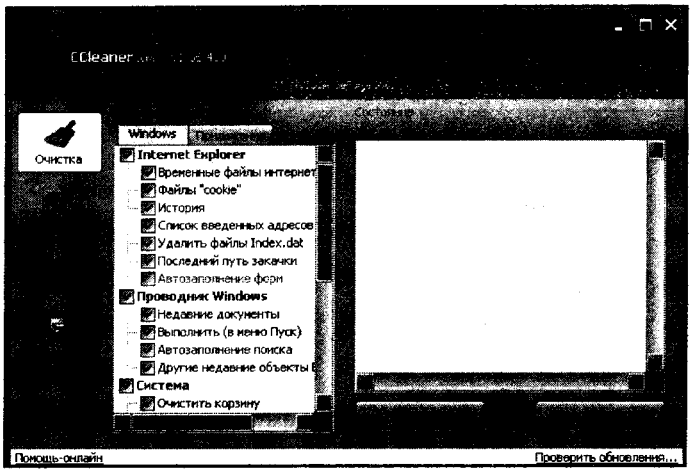
- Откройте ваш любимый поисковик и установите курсор на строчку запросов.
- Нажмите комбинацию клавиш **Alt** и «стрелка вниз».
- Для «промотки» открывшегося списка запросов пользуйтесь кнопками «стрелка вниз» и «стрелка вверх».
- Пролистайте список до запроса, от которого вы хотели бы избавиться, и удалите его с помощью кнопки **Del**.

Еще раз подчеркну, что этот метод работает с ЛЮБЫМИ формами на веб-сайтах, и пользоваться им куда удобнее и рациональнее, чем удалять все данные форм скопом. В конце концов, «криминальных» запросов обычно бывает немного...

С «cookies» история будет несколько сложнее. Полностью запретить браузеру сохранять их, конечно, можно (через пункт ***Файлы Cookie*** меню ***Сервис ▸ Свойства обозревателя ▸ Безопасность ▸ Другой)***, но в результате этого многие страницы Сети не будут корректно отображаться на вашем компьютере, а некоторые сайты отсутствие «пирожков» будет в буквальном смысле слова сводить с ума. Поэтому специалисты по безопасности рекомендуют «отсекать» нежелательные «пирожки», если уж возникла такая необходимость, при помощи дополнительных утилит типа **Anonymous Cookie** (http://www.luckman.com) или другой программы этого типа.

Очистка истории работы в Сети — дело «чистильщиков» — например, **TuneUp Utilities 2007**, System Mechanic или абсолютно бесплатной, но умелой «чистилки» CCleaner (http://www.ccleaner.com). Она может удалить как все «следы» скопом (Журнал, cookies, список URL в адресной строке браузера, историю запросов поисковых систем), так и выборочно.

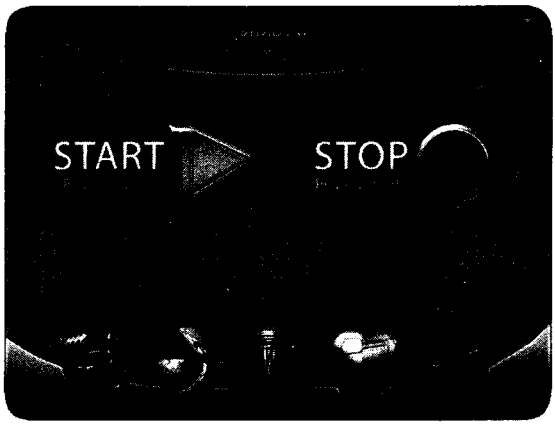
Если же вы не хотите постоянно терзаться мыслями — забыл я удалить историю своих похождений или нет? — то вас выручит бесплатная программка под названием **Free History Eraser** (http://smartprotector.com/eraser/). Ее можно настроить так, что она сама будет очищать историю адресной строки при каждом выходе из браузера или при перезагрузке Windows.



CCleaner

Впрочем, даже самый отъявленный параноик не думает о приватности постоянно. Скорее — время от времени, в момент посещения каких-либо сайтов, которые по каким-либо причинам нежелательно являть на глаза посторонним. А для таких случаев все уже знакомые нам меры — вроде лихорадочной зачистки журнала и сохраненных форм — становятся уж слишком хлопотными. Вот если бы можно было становиться «невидимкой» на время, без всякой возни с настройками...

Почему бы и нет? С программой **Shadow Professional** это не составит никакого труда. Достаточно лишь нажать на кнопку Start — и вы тут же переходите в «теневой» режим: история ваших путешествий в Журнале браузера не фиксируется и никаких следов на компьютере не остается.



Shadow Pofessional

Впрочем, это далеко не все: с помощью «тени» можно создавать на компьютере папки и файлы-невидимки – например, секретный раздел в вашей папке «Избранное», зайти в который сможете только вы. Ну и в довесок «тень» может поработать и неплохим чистильщиком, тщательно удалив историю браузера и прочие следы ваших сетевых странствий.

АПТЕЧКА: НА ВСЕ СЛУЧАИ ЖИЗНИ

Безопасность в Интернете

До чего же парадоксальна человеческая натура! Ведь каждый божий день мы слышим о все новых и новых кознях хакеров, меланхолично фиксируем появление новых вирусов, сокрушаемся по поводу нестабильности и уязвимости существующих информационных систем... И в то же время не делаем ничего, чтобы хоть как-то обезопасить свой собственный компьютер! Более того – даже не знаем, какие именно опасности могут нам встретиться на информационной магистрали.

А их не так уж мало. При всем своем внешнем дружелюбии дорога Интернет отнюдь не вымощена желтым кирпичом, на ней и ухабы не редкость, да и замаскированные ямы с кольями на дне попадаются. Другое дело, что для многих «хищников» наш брат пользователь – слишком мелкая

дичь. И потому на ваш компьютер, подключенный к Сети в сеансовом режиме, через слабенький модемный канал, вряд ли станут покушаться серьезные хакеры. Из тех, которых хлебом не корми, а дай «завалить» серьезный сервер какого-нибудь Пентагона. И содержимое вашего винчестера не улетит за считаные секунды в бездну Интернета (этот потрясающий пассаж автор вычитал в опусе одного из мэтров отечественной фантастики), «вытянутое» тем же загадочным «взломщиком».

Все это – опять-таки, для нас, пользователей – не страшнее бумажного тигра. Однако и настоящих тигров не так уж мало, и встреча с ними вам в большинстве случаев никаких приятных эмоций не доставит.

Поэтому о защите подумать не помешает. Но прежде все-таки надо узнать, от чего именно мы будем защищаться. Так что пересчитаем и поименуем имеющуюся полосатую нечисть.

С вирусами и троянскими программами мы уже свели знакомство в самом начале книги. Таким образом, у нас остаются лишь две проблемы – Приватность и Безопасность.

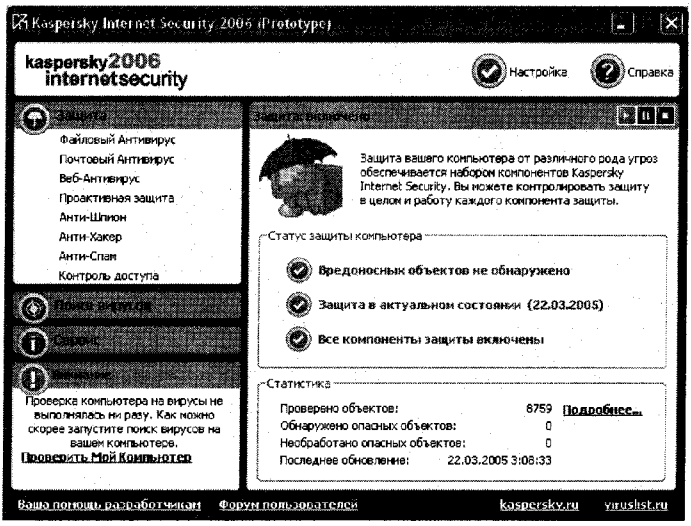
Понятие Приватности подразумевает, что вы, как пользователь, имеете полное право быть защищенным от наблюдения за вашими действиями извне – пусть даже ничем противозаконным вы не занимаетесь.

Понятие Безопасности включает возможность защититься от не санкционированного вами проникновения на ваш компьютер.

Многофункциональные пакеты

Kaspersky Personal Security Suite (http://www.kaspersky.ru)

Назвать программу «Лаборатории Касперского» лучшим россйиским продуктом одним из са-



Kaspersky Personal Security Suite

мых надежных «сторожей» в мире – значит всего лишь в очередной раз озвучить прописную истину. Как бы мы не относились к аппетитам «Касперского» по части процессорных ресурсов и памяти, его надежность в любом случае остается вне всяких сомнений. Во всяком случае, среди интегрированных продуктов поспорить с «Касперским» может лишь Norton Internet Security, который грузит ваш компьютер значительно больше.

В состав программы входят антивирус, брандмауэр, антиспам-фильтр и модуль защиты от шпионских и реклманых программ (antispyware). С антивирусом мы уже знакомы, что же касается файрвола, то он, конечно, несколько уступает по возможностям тому же Outpost. Однако для тех, кто хочет не постоянно что-то подкручивать в настройках, а просто работать, его возможностей хватит с лихвой. Спам-модуль, на мой взгляд, работает вполне корректно. Модуль же Antispyware – новичок, появившийся лишь в шестой версии продукта, также работает, как минимум, не хуже западных продуктов аналогичного класса.

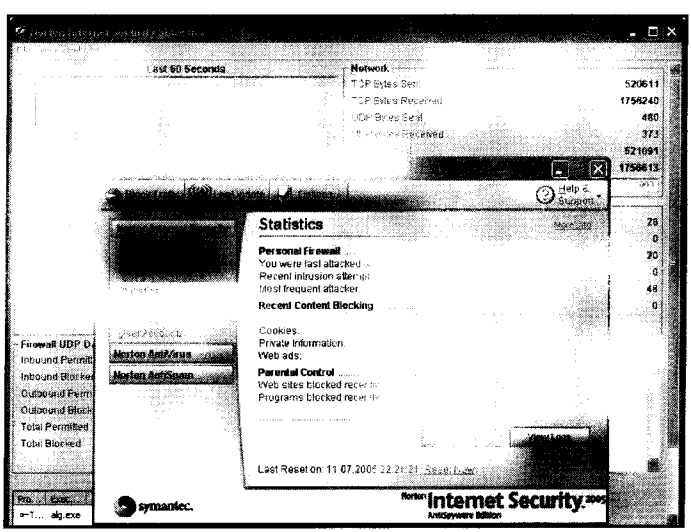
Подытожим. Конечно, можно попытаться создать более эффективный щит, установив на компьютер «связку» из нескольких различных программ. Однако и обойдется она вам гораздо дороже, да и на быстродействии скажется не лучшим образом. Kaspersky Internet Security –

решение, как минимум, хорошо сбалансированное и неплохо зарекомендовавшее себя. Для домашнего компьютера – возможно, лучший выбор.

Norton Internet Security

(http://www.symantec.com)

Сердцем этой программы, бьющемся в тесной «оболочке» коммерческого продукта, стала некогда компактная и условно-бесплатная программа ATGuard – бесспорный чемпион рынка файрволлов пятилетней давности. Взлет этого продукта был настолько стремительным, что могущественная Symantec поспешила перекупить взрослею-



Norton Internet Security

щего на глазах конкурента, выпустив его под новым именем почти без изменений.

Продукты Symantec имеют большие возможности конфигурации: теперь вы можете не просто установить безликий «уровень защиты», но и попробовать самостоятельно разобраться с несколькими десятками(!) потенциально опасных действий. Одни из них стоит безусловно запретить, другие – ограничить, третьи – разрешить без всяких оговорок. Безусловно, разбираться с настройками NIS с непривычки затруднительно, однако доступный и удобный интерфейс значительно облегчает эту задачу. Кстати, «семейная» модификация Norton Internet Security позволяет создать помимо общих «правил» и индивидуальные настройки для всех членов вашей семьи.

Помимо уже знакомых нам «троянцев» и атак на порты, продукты Symantec моментально разбираются с опасным содержанием интернет-страничек – скриптами и аплетами. Программа умеет шифровать системные пароли. Уверенно собирает в свою корзинку все сваливающиеся из Сети «печенья» (Cookies).

Количество перехваченных атак, высвечиваемое на информационном табло программы, приводит непосвященного в состояние легкого ступора: создается впечатление, что на ваш компьютер ополчилось сразу несколько злобных и

настойчивых хакеров. И только после разъяснений знатоков, что большая часть этих «атак» – не что иное, как обычный «сетевой шум», мусор, – на душе становится намного легче. В любом случае, нападения извне программа отражает бесподобно, хотя с атаками изнутри тот же ZoneAlarm справляется удачнее.

Один из главных козырей программ, построенных на основе ATGuard – способность убивать всплывающие рекламные окна и даже вырезать со страниц баннеры! В итоге работа становится не просто безопасной, но и быстрой – сами знаете, сколько времени уходит на загрузку из Сети всяческих рекламных «дополнений».

Программа умеет распознавать баннеры, принадлежащие к крупнейшим рекламным сетям. Но если вовремя выявить и прибить какую-нибудь надоедливую картинку не получилось, не беда – ее всегда можно добавить в базу данных, перетащив мышкой в специальную «корзинку».

Norton Internet Security может выступить в роли «сетевой няньки», позволяя родителям защитить детей от случайного (или намеренного) визита на страницы, содержащие неподходящую для этого возраста информацию. Впрочем, именно эта функция программы едва ли будет затребована большинством пользователей, поскольку аналогичное (хотя и чуть менее мощное) средство за-

щиты встроено в сам Internet Explorer (меню ***Сервис ▸ Свойства обозревателя ▸ Содержание ▸ Ограничение доступа***).

В последнюю версию Internet Security 2004 включен и модуль Norton AntiSpam, который позволяет вам блокировать навязчивую рекламную почту. Справедливости ради стоит сказать, что способности именно этого компонента не вызывают особых восторгов: хотя AntiSpam и построен на основе модного нынче алгоритма Bayesian, с изобличением рекламных писем он справляется значительно хуже, чем, например, бесплатная программа на основе того же «движка» – SpamPal (http://www.spampal.org).

Norton AntiSpam умеет работать совместно с вашей почтовой программой – например, Outlook Express. Здесь AntiSpam создает специальную папку, куда и перемещает все сомнительные письма. Если вы уверены, что нужное письмо попало в «мусорную» папку случайно, щелкните по нему правой кнопкой мышки и восстановите через контекстное меню.

Наконец, Norton Internet Security умеет бороться с вирусами – не самостоятельно, конечно, а с помощью встроенного пакета Norton Antivirus, который Symantec упорно встраивает едва ли не в каждый свой продукт. Во многом за счет этой «полезной добавки» программа значительно разбухла в размерах (до 70 Мб в сравнении с 3 Мб старого

ATGuard), что не лучшим образом сказалось на ее быстродействии.

Если говорить коротко, то Norton Internet Security – лучший «защитник» для пользователей-новичков. Как и положено всем продуктам Symantec, программа стремится все делать самостоятельно – долгая возня с настройками тут не приветствуется. Наоборот, механизм тонкой настройки запрятан глубоко в недра программы и, чтобы самостоятельно заблокировать порты, вам придется поискать этот «пульт управления» как следует. Возможно, оно и правильно...

В качестве компенсации своей тяжеловесности Norton Internet Security представляет пользователю максимум удобств – он и от вирусов спасет, и от хакеров, и рекламные письма изничтожит... Классическая домашняя программа – что сказать еще?

McAfee Internet Security Suite

(http://www.mcafee-at-home.com)
(http://www.mcafee.ru/products/homepc/)

Как и пакет от Symantec, защитный комплект пакет от McAfee включает полный набор утилит для обеспечения безопасности в сети:

- McAfee Personal Firewall – персональный брандмауэр.
- McAfee VirusScan – антивирус.
- McAfee Spam Killer – программа для борьбы с рекламными письмами.
- McAfee Privacy Service – защита вашей конфиденциальной информации при работе в Сети.

Если сравнивать McAfee Firewall с Norton Personal Firewall, то можно выделить несколько основных моментов: во-первых, программа от McAfee работает несколько шустрее, а во-вторых, отличается гораздо большим самомнением. По сути дела, пользователю предоставляется элементарный выбор – пускать данную программу в сеть или не пускать? Norton работает куда тоньше, позволяя конкретизировать, по каким адресам программа имеет право «ломиться», а по каким – нет. Впрочем, программа вполне уверенно отлавливает действия простых «троянцев», а заодно блокирует попытки проникнуть в компьютер извне. Для домашнего пользователя этого вполне достаточно.

Кстати, забавно, что обе эти программы созданы сторонними разработчиками: в основе Norton Personal Firewall, как известно, лежит «движок» от AtGuard, а программа McAfee основана на механизме другого «сторожа» – ConSeal Private Desktop.

Основные функции программы (по информации разработчика):

- Обнаружение вторжений из Интернета – позволяет обнаружить основные типы сетевых атак и другой подозрительной активности с возможностью блокировать любое дальнейшее взаимодействие с атакующим.
- Сканирование ПК на предмет наличия программ, имеющих возможность выходить в Интернет, с целью создания разрешающих или запрещающих правил и минимизации числа последующих предупреждений.
- Обнаружение клавиатурных шпионов и других маскирующихся программ.
- Поддержка Internet Connection Sharing (ICS) и Network Address Translation (NAT).

Кстати, о функциях. Как водится, целое оказывается больше суммы его составляющих. Базовые таланты вошедших в комплект программ дополняются рядом новых возможностей:

- Блокирование рекламы – увеличивает скорость работы в Интернете.
- Обнаружение и фильтрация Web Bug – предупреждает о возможных попытках кражи информации.

- Обнаружение клавиатурных шпионов и других маскирующихся программ.
- Управление и блокирование Cookies – позволяет управлять нужными и удалять ненужные Cookies.
- Возможность многопользовательского конфигурирования – позволяет задавать различные настройки для каждого пользователя ПК.

Антивирусные программы

Вирус – едва ли не главный враг компьютера. Крохотные зловредные программки могут в одночасье испортить плоды вашего многомесячного труда, уничтожить текстовые файлы и электронные таблицы, а то и вообще испортить файловую систему на жестком диске...

Ведут себя компьютерные вирусы точно так же, как вирусы живые: они прячут свой код в теле «здоровой» программы и при каждом ее запуске активируются и начинают бурно «размножаться», бесконтрольно распространяясь по всему компьютеру.

Это – одна сторона деятельности вируса. Не самая страшная, кстати. Если бы вирус просто размножался, не мешая работе программ, то с

ним, наверное, не стоило бы и связываться. Тем более, что значительное число существующих вирусов принадлежит именно к этой, относительно безвредной категории.

Но, помимо размножения, у вируса есть еще и другое «хобби» – разрушать, пакостить. Степень «пакостности» вируса может быть разная – одни ограничиваются тем, что выводят на экран навязчивую картинку, мешающую вашей работе, другие, особо не раздумывая, полностью уничтожают данные на жестком диске.

Как и обычные вирусы, вирусы компьютерные – паразиты, для размножения им нужен «носитель»-хозяин, здоровая программа или документ, в тело которой они прячут участки своего программного кода. Сам вирус невелик – его размер редко измеряется килобайтами. Однако натворить эта «кроха» может немало. В тот момент, когда вы, ничего не подозревая, запускаете на своем компьютере зараженную программу или открываете документ, вирус активизируется и заставляет компьютер следовать не вашим, а его, вируса, инструкциям. Современные вирусы исхитряются портить не только программы, но и «железо». Например, вчистую уничтожают содержимое BIOS материнской платы или калечат жесткий диск.

Сегодня науке известно около семидесяти тысяч компьютерных вирусов – маленьких вредо-

носных программок, следующих в своей жизни только трем заповедям – Плодиться, Прятаться и Портить. Или, по, крайней мере, первым двум из них.

Разновидностей компьютерной «нечисти» тоже немало. Однако чаще всего пользователям стоит опасаться следующих:

Макровирусы. Представляют собой микропрограммы, написанные на языке VBA, встроенном в приложения популярных офисных пакетов. Паразитируют на документах Microsoft Office – зараженным может оказаться внешне безобидный текстовый документ или электронная таблица. Распространяются макровирусы и в виде отдельных файлов-макросов с расширением *vbs*. К счастью, новые версии программ Microsoft Office (Word, Excel) снабжены встроенной защитой от макровирусов – возможно, именно поэтому поголовье вирусов этого типа сегодня значительно уменьшилось.

«Программные» (исполняемые) вирусы. Это – обычные программные файлы с расширением *exe*, которые вы можете получить в виде вложения в электронное письмо.

«Троянские» программы, в отличие от «чистых» вирусов, порчей данных не занимаются. Чаще всего, попав в компьютер, они ведут себя тихо и скромно, но навредить могут куда силь-

нее обычных вирусов. «Троянцы» крадут ваши личные данные (начиная от пароля для доступа в Сеть и заканчивая номерами кредитных карточек) и незаметно переправляют их своим создателям. Заразиться «троянцем» можно как через электронное письмо, так и получить его «в нагрузку» к скачанной из Интернета программе.

Полностью «отсечь» вирусы от вашего компьютера вряд ли удастся, разве что вы удалите из системы дисковод, перестанете работать в Интернете и будете пользоваться только легальным программным обеспечением. Но в наших условиях все эти советы – особенно последний – выглядят либо утопией, либо издевательством.

Остается один способ: снабдить вашу ОС надежными сторожами – антивирусными программами, которые смогут вовремя распознать и обезвредить прокравшегося в ваше логово врага.

Практически все программы, упомянутые в нашем обзоре, просты и удобны в пользовании, способны отлавливать практически все существующие сегодня группы вирусов (за исключением «троянцев» – этот «орешек» оказался по зубам лишь немногим антивирусным пакетам). Большинство антивирусов способны не просто проверять по запросу пользователя диск на наличие вирусов, но и вести незаметную проверку всех запускаемых на компьютере файлов. Наконец, все

современные антивирусы снабжены механизмом автоматического обновления антивирусных баз данных через Интернет.

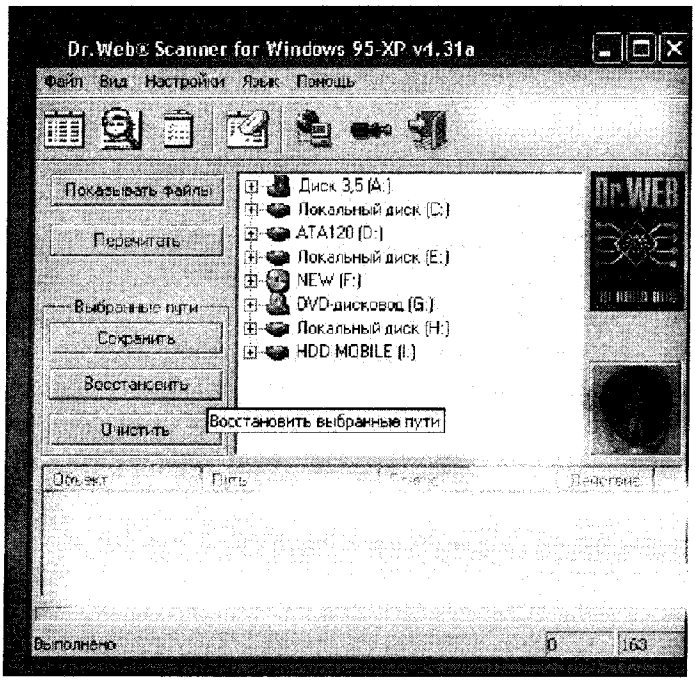
Получается, правильный выбор – дело вкуса? Возможно, что так оно и есть. Во всяком случае, существует несколько основных точек зрения на эту проблему.

Ряд пользователей считает, что нет ничего лучше отечественных продуктов, наиболее приспособленных к нашей вирусной «атмосфере». Не стоит сбрасывать со счетов и патриотизм – анекдотично, но даже пользователи пиратских копий отечественных антивирусов свято верят в то, что вносят свой вклад в поддержку российских производителей.

Другая группа пользователей ориентируется на результаты тестов авторитетных западных изданий – и в первую очередь, на хит-парад Virus Bulletin 100% Awards (http://www.virusbtn.com/100/). Кстати, отечественные антивирусы KAV и Dr.Web неизменно присутствуют в Top10 самых надежных антивирусных программ этого рейтинга, хотя на первых местах неизменно оказываются продукты, о которых наши пользователи и слыхом не слыхивали. А единственная по-настоящему популярная в России западная программа – Norton Antivirus – неизменно плетется в хвосте списка (что не мешает этой программе получать множество других авторитетных премий)...

Dr.Web

(http://www.drweb.ru)



Dr.Web

Более семи лет назад, в эпоху DOS, Dr.Web мог с полным правом считаться первым и лучшим среди российских антивирусов. Однако запоздание с переходом на Windows-версию сыграло роковую роль: популярность Dr.Web стала стремительно падать... И лишь относительно недавно, после подорожания «всенародно любимого» AVP (сменившего к тому времени название на KAV),

интерес к разработке Игоря Данилова вновь вырос. И оказалось, что этот «вечно второй» продукт в большинстве случаев может предложить не худший уровень защиты, чем его коллега «от Касперского».

Антивирусная база Dr.Web почти вдвое меньше, чем у KAV (на момент написания книги – около 30 тысяч записей). Однако создатели уверяют, что на результатах тестирования это не сказывается, поскольку в Dr.Web реализован принципиально иной подход, чем в его коллегах-антивирусах: в программу встроен модуль эвристического анализатора, который позволяет обезвредить не только уже известные программе и занесенные в базу данных, но и новые, еще не опознанные вирусы. В любом случае, малый размер и сравнительно небольшой объем базы не мешают Dr.Web регулярно занимать призовые места в антивирусных «чемпионатах» и сравнительных тестированиях. Кроме того, скорость пополнения баз данных у обоих антивирусов примерно одинакова.

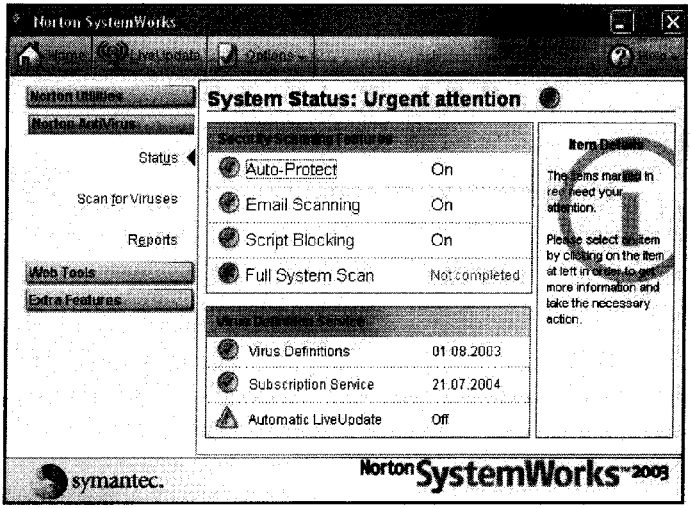
Как и KAV, Dr.Web устроен по модульному принципу: сканированием диска занимается базовая программа, а контролем запускаемых программ и документов – модуль Spider. Проверяются все категории файлов, которые могут быть заражены: исполняемые файлы, документы Microsoft Word, архивы всех популярных форматов (ARJ, ZIP, RAR, TAR и т. д.), скрипты VBS и многие другие.

По заявлениям разработчиков, надежность программы можно повысить, используя совместно с Dr.Web «ревизора диска» ADinf от фирмы «Диалог-Наука».

Norton Antivirus

(http://www.symantec.com)

Norton Antivirus является «самым-самым» сразу по целому ряду позиций. Самый красивый, самый логично устроенный. Обладатель самой большой базы данных вирусов. И – увы! – самый массивный, неповоротливый и требовательный к ресурсам.



Norton Antivirus

Norton Antivirus – программа на редкость «въедливая», из-под ее контроля не уйдет ни один запущенный на компьютере процесс. После установки Norton Antivirus (например, в составе комплекта Norton System Works) о ней можно вообще забыть – NAV сама проконтролирует все что нужно.

В частности, этот антивирус умеет перехватывать сообщения электронной почты на полпути к вашему почтовому ящику и обрабатывать их (не забывая продемонстрировать свой труд в поте лица пользователю). Почту, уходящую от вас, программа тоже проверяет – на всякий случай. Конечно, обезвреживать почтовые вирусы умеют и другие программы, но только при открытии вложений, NAV же делает это заранее. Кроме того, NAV встраивает защитный механизм в приложения Microsoft Office, контролируя каждый открываемый на компьютере документ... Последние версии Norton Antivirus умеют обнаруживать не только вирусы, но и некоторые «троянские» модули.

Идеология программы – совать свой антивирусный нос во все подряд, не затрудняя себя экономией системных ресурсов, а пользователя – работой с настройками программы. «Папочка сам знает, что тебе лучше!» ...Может быть, и вправду знает. В конце концов, стать «стандартом» для всего мира только за красивые глаза было бы невозможно.

Все эти процессы будут протекать для пользователя невидимо, и привлекать ваше внимание программа будет лишь в момент обнаружения нового вируса или при необходимости обновить антивирусные базы через Интернет. Кстати, вирусная база NAV, пожалуй, не имеет конкурентов по числу распознаваемых вирусов – около 55 000!

Увы – Norton Utilities остается лидером не только по простоте работы, но и по медлительности. Этот тяжеловес занимает рекордный объем в оперативной памяти компьютера, а его встроенные «сторожа» существенно замедляют скорость работы с электронной почтой и офисными документами. Наконец, традиционно неудобен «нортоновский» механизм обновления – дополнения к «Касперскому» выходят гораздо чаще, к тому же они существенно меньше по размерам, да и канал связи с сервером Symantec работает гораздо хуже.

Зато есть у NAV и завлекалочки, на которые охотно клюют пользователи-новички. Программа не заставляет вас разбираться с многочисленными настройками, все просто и удобно. Установил раз – и забыл... Кроме того, встроенные «сторожа» предоставляют вам новые возможности – так, при обнаружении зараженного письма NAV позволяет не просто удалить его или попытаться вылечить, но и переместить в карантин.

Наконец, «на руку» программе играет и тот факт, что Norton Antivirus поставляется (вместе с Norton Utilities и Norton CleanSweep) в составе популярного утилитного комплекта Norton System Works, который сегодня является обязательным элементом программной «начинки» любого компьютера. И стоимость этого комплекта вполне сопоставима с ценой отдельной(!) антивирусной программы. Кроме того, Norton Antivirus можно приобрести в составе еще одного комплекта Symantec – Norton Internet Security Professional, в состав которого входит также одноименный файрволл.

Panda Antivirus

(http://www.viruslab.ru)

Этот испанский антивирус в последнее время активно распространяется и на российских просторах. Его преимущества – отлично сработанный интерфейс (одни звуковые эффекты чего стоят!), поддержка русского языка и отличное сопровождение. Недостаток – подобно программам от Symantec, Panda не слишком дружелюбно относится к любителям «тонкой настройки».

«Это самый удобный антивирусный пакет для домашнего использования – Titanium специально разрабатывался для тех, кто не является

профессионалом в области информационных технологий. Программа работает по принципу «установил и забыл».

Titanium автоматически, то есть быстро и незаметно для пользователя, пополняет свои антивирусные базы при каждом подключении к Интернету. Благодаря новому сверхбыстрому механизму проверки UltraFast, не имеющему себе аналогов в мире, программа работает с максимальной скоростью при минимальном использовании ресурсов компьютера. Эксклюзивная технология SmartClean, использованная в Panda Antivirus Titanium, может восстанавливать работоспособность и корректные параметры системы в случае их повреждения рядом наиболее распространенных вирусов.

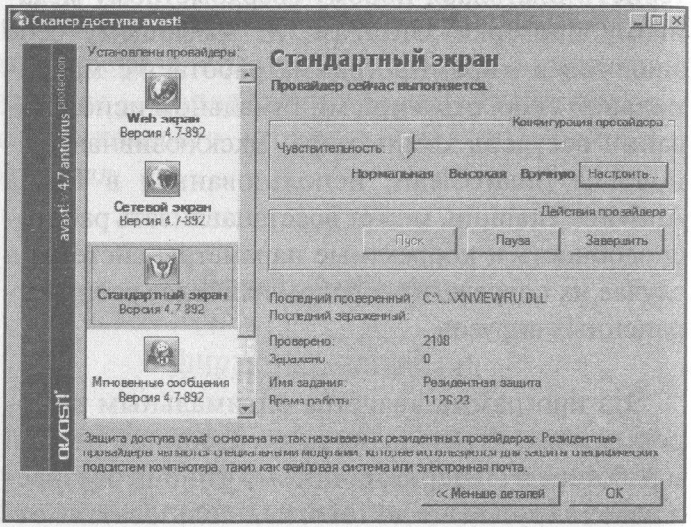
Эта программа является оптимальным выбором для тех, кто пользуется электронной почтой и работает в Интернете, потому что она обезвреживает вирусы еще до того, как пользователь открывает зараженное письмо. Titanium совместим с наиболее широко используемыми на рынке почтовыми клиентами – Microsoft Outlook, Outlook Express, Eudora, Pegasus, MSN Mail, Netscape Mail.»

Реклама рекламой – а в Панде действительно много интересного. Например, этот зверь умеет лечить файлы внутри архивов, на чем спотыкается даже умелый Norton. Панда не му-

чает новичков многочисленными вопросами – она просто тихо делает свое дело. Да и обновляется оперативно...

Avast

(http://www.avast.ru)



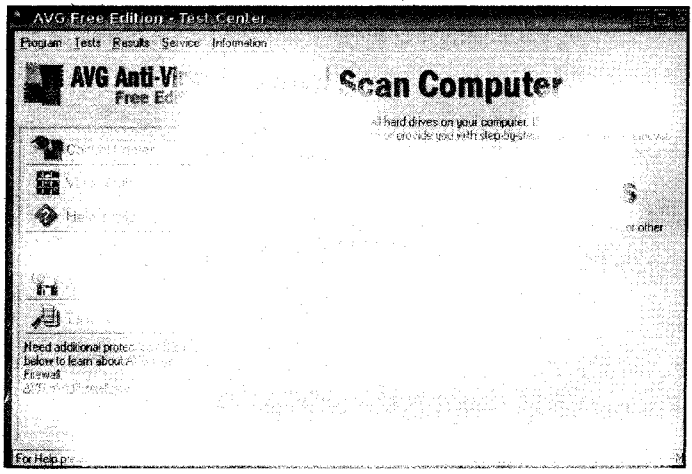
Avast

Бесплатный антивирус – вещь в наше время не менее редкая, чем говорящая лошадь. Но отдельные экземпляры этого редкого представителя фауны еще встречаются. И вот перед вами один из них – «домашний» вариант довольно известного антивирусного пакета. Ко всему прочему – еще и русскоязычный.

От профессиональной версии программы бесплатный avast отличается не так уж и сильно: он отстает от коммерческих антивирусов разве что в области работы со скриптами, adware и spyware. Но от самых распространенных вирусов он спасет, в том числе – и тех, что распространяются через электронную почту, через интернет-пейджеры и файлообменные системы. К тому же он быстр, занимает немного места в памяти... Словом – отличная аптечка на тот случай, если более умелого «доктора» по каким-то причинам не найдется под рукой...

AVG Antivirus

(http://www.grisoft.com)



AVG Antivirus

Бесплатный антивирус от чешской компании Grisoft – один из первых и самых известных представителей этого класса. К сожалению, русский интерфейс в этой программе отсутствует, к тому же базы данных антивируса необходимо обновлять вручную (что сводится к простому нажатию кнопки «Обновить»). Зато уровень защиты у этой программы достаточно высок: программа напрочь отсекает от системы классические вирусы, популярные «трояны» и даже кое-что из spyware-модулей. Значительно хуже обстоит дело с руткитами, но это – ахиллесова пята практически всех бесплатных антивирусов. Зато AVG Antivirus отличается едва ли не самыми скромными требованиями, что делает его идеальным антивирусом для ноутбуков. Кстати, на сайте AVG вы можете найти еще одну бесплатную программу, предназначенную для удаления spyware и adware-модулей.

Remove It!

(http://www.incodesolutions.com)

Бесплатный антивирусный сканер. В отличие от обычных антивирусов, он не имеет резидентного модуля, который может «висеть» в памяти постоянно, и не поддерживает обновление баз — они встроены в саму программу. Для постоянного мониторинга системы программа не годится, однако с ее помощью можно быстро очис-

тить зараженную систему от вирусов (только не забудьте заранее скачать из Сети последнюю версию!)

Clrav

(ftp://ftp.kaspersky.ru/utils/clrav.com)

Конечно, полноценный и надежный антивирус – лучшее «лекарство»... Хотя нет, лекарство-то мы принимаем уже во время болезни, а вот установка антивируса на уже зараженный компьютер поможет далеко не всегда. Особенно в том случае, если ваша «персоналка» ухитрилась подхватить модную нынче «червивую» хворь.

Тут надо действовать быстро и оперативно, и времени на поиск полноценной программы уже не остается. Специально для таких экстренных случаев Лаборатория Касперского разработала компактную и бесплатную программу Clrav.

Интерфейс у программы самый непритязательный – точнее, его нет вовсе. Однако этот сканер может за несколько минут обнаружить и обезвредить около 20 разновидностей червей – в том числе самых злокозненных семейств Goner, SirCam, Navidad, BleBla, Klez и многих других.

Clrav полезно регулярно запускать даже обладателям полноценных антивирусов – эта утилита

вытаскивает из потаенных нор даже самых хитрых червей, добраться до которых не смогли другие программы.

Не забывайте, что, как и обычный антивирус, Clrav регулярно обновляется – примерно раз в два месяца вы сможете скачать с сервера Лаборатории Касперского его новую версию.

Защита от «троянских» программ

Наряду с уже хорошо знакомой нам вирусной угрозой стали говорить об опасности, исходящей от программ другого типа – программ-«троянцев». Они распространяются через те же каналы, что и вирусы: «троянец» может нанести вам визит в виде вложения в электронное письмо, просочиться через защиту браузера или обосноваться в дистрибутивном комплекте скачанной вами программы.

«Трояны» задумывались как программы, которые помимо своей основной работы решали еще какую-то скрытую от взора пользователя задачу. Примером «троянца» можно считать неоднократно описанную в различных (полу)фантастических рассказах ситуацию, когда какая-то корпоративная программа, не обнаружив в платежной ведо-

мости фамилию программиста, ее написавшего, начинала всячески «шалить».

В старые времена «трояны» писались именно как некие дополнительные функции какой-то основной программы.

Напомним, что сегодняшние «троянцы» чаще всего занимаются тем, что воруют пароли для доступа в Интернет и другую «секретную» информацию (например, номера кредитных карточек) и пересылают ее «хозяину». Такими же темными делами занимаются и «кейлоггеры» — программки, которые втихаря отсылают своему автору информацию о том, по каким именно клавишам вы щелкали в течение всего дня. Нетрудно догадаться, что из этой текстовой мешанины можно легко выудить и номера кредиток, и пароли к сайтам или почтовому ящику.

Установка различных серверов для удаленного управления и открытие «черных ходов» для доступа к вашей системе — другой распространенный вид «сетевой заразы». Этим занимаются самые опасные разновидности вредительских программ — «руткиты», «трояны-невидимки», которые умеют так хитро маскироваться в системе, что обнаружить их присутствие фактически невозможно. Если подобный «зверь» оказался у вас в системе, то его хозяин сможет работать на вашем компьютере почти как на своем собственном. Существуют и другие виды руткитов, которые могут, к при-

меру, заблокировать на вашем компьютере запуск определенных программ. И снова вспомним, что в распространении подобной заразы была уличена даже компания Sony. В 2005 году в музыкальном мире разразился грандиозный скандал после того, как на выпущенных этой компанией «защищенных от копирования» CD была найдена программа-руткит. Она незаметно устанавливалась на компьютер в момент загрузки диска и препятствовала его копированию – а заодно и нарушала работу всей системы. Вал исков заставил Sony признать свою вину и изъять из продажи все зараженные CD... Но откуда нам знать, не последовал ли кто-то ее примеру? Ведь руткиты тем и опасны, что их практически невозможно обнаружить.

Самое главное: всегда с подозрением относитесь к файлам, полученным из незнакомого источника. Да и из знакомого – тоже. Любой файл, полученный по почте, если вы заранее не договаривались о его отправке вам запросто окажется «трояном». Большинство так называемых «хакерских» программ, предназначенных для взлома сети и т.п. – тоже окажутся «троянами». Здесь очень хорошо срабатывает правило: «То, что у вас паранойя, еще не значит, что за вами не следят».

Невредно напомнить, что довольно часто «троянца» можно определить и по стилю письма. Если вы получаете письмо, или видите на страничке что-то вроде «эй, чувак, здесь самая крутая нюка», то процентов 90, что это именно «троян».

PestPatrol

(http://www.pestpatrol.com)

Одна из лучших разработок для защиты от «троянских» программ.

PestPatrol – это мощное средство защиты, которое выявляет и удаляет различных разрушительных «паразитов», таких, как «трояны», программы слежения, хакерские программы и им подобные. Программа дополняет такие средства информационной защиты, как антивирусы и файрволлы, расширяя границы защиты и распространяясь на программы, которые, по сути, вирусами не являются, но могут нанести вред вашему компьютеру и вторгнуться в ваше личное пространство.

Trojan Remover

(http://www.simplysup.com/tremover/)

Как известно, далеко не все традиционные антивирусы способны отлавливать и обезвреживать «троянские» программы. Небольшая утилита от Simply Super Software – одна из немногих, созданных специально для борьбы с «троянцами». При запуске программа сканирует реестр и INI-файлы Windows в поисках подозрительных модулей. Если найденные программы числятся в базе данных

как «троянцы», они будут удалены. В сомнительных случаях программа предоставляет выбор самому пользователю.

С программой поставляется база на 16 000 сигнатур вредных программ. К сожалению, базы данных Trojan Remover обновляются не слишком часто, что несколько снижает эффективность программы.

Защита от Spyware и Adware

Незваный гость, как известно, хуже врага – пусть даже он и не пакостит особо, а просто торчит в вашем доме, оттягивая на себя внимание и без конца встревая в вашу жизнь.

Как уже было сказано, это не вирусы – хотя по злокозненности наши «герои» схожи с этой заразой: вашей информации повредить они не могут, а вот по назойливости им равных нет. «Шпионские» и рекламные модули, снабжающие своих создателей информацией о вашей работе, заодно «подкармливают» вас изрядной порцией ненавязчивых (а иногда – и ОЧЕНЬ даже навязчивых) советов и заманчивых предложений.

Как такое может произойти? Да вспомним ту же историю со смайликами: заходите вы на незнакомый сайт, который тут же предлагает вам АБСОЛЮТНО БЕСПЛАТНО установить в компьютер программу для вставки в письма и сообщения вашей «аськи» крутейших анимированных смайликов. Выглядят они действительно очень круто: катаются по экрану, подмигивают, строят рожицы и даже порой издают какие-то звуки. Вы щелкаете на кнопку ***Установить*** – и действительно, искомые смайлики скачиваются, и устанавливаются, и ваш антивирус молчит как партизан... Все вроде бы нормально! Отнюдь: через несколько минут вы замечаете, что проклятые смешинки заставляют ваш браузер при каждом открытии заходить на их сайт, который тут же начинает засыпать вас рекламой. Вы меняете страничку – и все равно после перезагрузки все возвращается на круги своя. Убить эту заразу нет никакой возможности, как удалить ее – неизвестно...

Если вы когда-то чисто случайно зашли на какой-то хитрый сайт, может произойти точно такая же история. Страница просто пропишет себя во всех возможных настройках вашей операционной системы. Наконец, рекламную начинку нетрудно подцепить вместе с какой-нибудь условно-бесплатной (или бесплатной) программой. Например, рекламными добавками напичкана даже всеобщая любимица ICQ – хорошо еще, что в настройки браузера она не лезет, а рекламу показывает лишь в своем собственном окне.Подоб-

ные неприятности могут подстерегать вас на сайтах интернет-казино, на сайтах с коллекциями «бесплатных» картинок и так далее.

Реклама, конечно, при всей своей надоедливости относительно безопасна. А вот «шпионские» модули (spyware) – штука куда более неприятная. Такой вот «шпионский» модуль – это тот же «троянец», но не «дикий», а приручённый хитрым хозяином того или иного сайта или разработчиком программы. Вреда от него вроде бы и нет, но... разве приятно осознавать, что за тобой постоянно наблюдает недреманное око Большого Брата. Или даже сотни глаз маленьких, но очень навязчивых «братцев»...

И, конечно, очень неприятно, если программа начинает наглеть и шпионить не только за собственными рекламными окошками, но и за тем, какие странички вы открываете в браузере (нечто подобное творит, например, популярная программа для хранения паролей Gator). Вот это уже не слишком приятно – хотя и реальной опасности также не представляет. Ведь в данном случае вся собранная информация идет не к спецслужбам, а все к тем же рекламщикам. Хотя и это тоже не слишком приятно.

Теоретически с рекламной и шпионской заразой должны справляться и обычные антивирусы – во всяком случае, самые продвинутые из них. На-

пример, тот же «Касперский» или Symantec Antivirus часто обезвреживают такие модули еще до проникновения на компьютер. Однако и они бессильны, если вы сами, добровольно, пустили в компьютер хорошо замаскированного «рекламного агента».

Так что поговорим о том, как максимально быстро и безболезненно вычистить из нашего компьютера всю эту окопавшуюся на нем нечисть. Сделать это порой не так просто, в особенности если речь идет о прописанных в системе рекламных модулях каких-нибудь порносайтов или казино..

Первым делом полностью очистите кеш своего браузера – это можно сделать как его собственными средствами:

Сервис ▸ Свойства обозревателя ▸ История просмотра ▸ Удалить ▸ Временные файлы Интернета (для Internet Explorer)

Также это можно сделать с помощью специальных программ-чистильщиков (CCleaner, WinTools.Net, TuneUp Utilities и куча других бесплатных и платных программ).

После этого скачайте и установите на компьютер специальную программу для «отлова» adware и spyware. А лучше – даже несколько.

AVG Anti-Spyware

(http://www.grisoft.com)

Если коммерческих «охотников» за spyware и adware на рынке пруд пруди, то хороших бесплатных утилит не так уж и много. Этим и воспользовалась чешская компания Grisoft, известная благодаря своему бесплатному антивирусу AVG: его «напарницей» и стала новая программа AVG Anti-Spyware. Этот сканер не отличается излишней щепетильностью по отношению к малоопасным модулям типа cookie (а именно на них, напомним, приходится львиный процент всех «тревожных звонков» того же Spyware Doctor) – их он находит гораздо меньше.

Однако по-настоящему к серьезным угрозам программа подходит ответственно. Единственная проблема – обновления для AVG выходят реже и позже, чем для коммерческих пакетов, к тому же бесплатная версия программы обновляется лишь в ручном режиме. Конечно, полноценная платная версия программы этих ограничений лишена, но покупать именно ее, на мой взгляд, не слишком оправдано. А вот бесплатная модификация довольно хороша для своей категории. Держать эту программу постоянно в памяти нет никакого смысла – все-таки при всех своих достоинствах она не лучшим образом сказывается на быстродействии компьютера... А вот регулярно проверять с ее помощью жесткий диск в режиме сканера не помешает.

Программы для защиты от «взломов» (файрволлы)

Итак, межсетевой экран или, как его чаще называют в обиходе, файрволл. В переводе на русский это слово (или его немецкий эквивалент – «брандмауэр») значит – «огненная стена». Вспомним двоякий смысл названия, – во-первых, преодолеть сплошную стену огня невозможно, если только ты не пожарник-профессионал. А с другой стороны, название это напоминает о хорошо известном способе тушения лесных и степных пожаров: навстречу надвигающейся огненной лавине пожарники пускают вторую, специально поджигая лес. Две огненные стены встречаются – и в мгновение ока уничтожают друг друга.

Таким же образом работают и компьютерные файрволлы, защищая наш компьютер от проникновения заразы извне. Непреодолимой стеной встают они на пути разрушающих программ и скриптов, а атаке через порты противостоят, пользуясь оружием самих нападающих – сканируя порты доступа.

При обнаружении попытки несанкционированного проникновения в ваш компьютер, программа может просто подать сигнал тревоги, а может сразу заблокировать доступ подкапывающе-

муся под вас «кроту». Это – основная функция всех программ этого класса, к которой, в зависимости от сложности продукта, добавлено еще множество других, более или менее нужных.

К сожалению придется огорчить всех тех, кто считает персональные файрволлы надежной защитой. Практика показывает, что большинство из этих программ-«стражей» довольно уязвимы, они могут отбить атаки лишь не слишком умелых хакеров. Они, увы, бессильны против настоящих профессионалов взлома. Если же вы хотите проверить, насколько «дыряв» ваш любимый файрволл, воспользуйтесь услугами утилит **Firewall Leakage Tester** и **Firehole**, которые вы сможете найти на большинстве сайтов по компьютерной безопасности.

Очень полезно напомнить, что существует и масса специализированных сайтов, которые позволят вам проверить защищенность вашего компьютера через Интернет. Например, такую услугу предлагает один из разделов корпоративного сайта Symantec (http://www.symantec.com/sabu/nis/nis_pe/)

Воспользовавшись одной из этих ссылок, вы можете проверить свой файрволл на уязвимость.

http://scan.sygate.com
http://www.auditmypc.com
http://www.pcflank.com/test.htm
http://www.hackerwatch.org/probe/

При этом многие современные «сторожа» выступают еще и в роли оптимизаторов и ускорителей. Помимо своей прямой обязанности, они умеют выполнять и ряд других полезных функций. Например, удаляют с сайтов рекламные баннеры, предотвращают появление многочисленных выпадающих рекламных окон. Вот почему автор позволит себе не согласиться с теми, кто утверждает, что в этих программах (в связи с их ненадежностью) и вовсе нет никакой нéобходимости.

Прибегать к услугам брандмауэров приходится даже пользователям Windows XP – притом, что в новых операционных системах Microsoft уже имеется встроенный брандмауэр. Его надежность порой даже выше, чем у отдельных программ этого типа, однако удобство работы со встроенным «сторожем» оставляет желать лучшего.

Напомним основные требования к современным файрволлам: они должны уметь отражать атаки не только извне (попытки сканирования портов), но и изнутри. Файрволл должен отслеживать активность установленных в вашей системе программ и позволять вам блокировать доступ к Сети любой из них.

Наконец, файрволл должен предоставлять вам возможность выборочного закрытия отдельных

портов (причем с учетом направления – «вход» или «выход», а также – конкретного протокола). Специально для пользователей домашних компьютеров, подключенных к скоростному выделенному каналу, еще раз приведем список портов, которые следует закрыть вручную (с указанием протокола доступа).

TCP:20,	TCP:445,
TCP:69,	UDP:445,
UDP:69,	TCP:555,
TCP:135,	TCP:4444,
UDP:135,	TCP:12345,
UDP:137,	TCP:54321,
TCP:139,	TCP:54320,
UDP:139,	TCP:65000

Конечно, «опасных» портов куда больше. Но это – тот необходимый минимум, который может уберечь вас от множества неприятностей. Специалисты по компьютерной безопасности и «продвинутые» пользователи могут заглянуть, к примеру, на сайт компании Commodon, где опубликован впечатляющий список потенциально опасных портов с указанием программ, которые их используют:

http://www.commodon.com/threat/threat-allports.htm

PortsLock

(http://www.smartline.ru)

PortsLock – это уникальный брандмауэр (файрволл), который полностью интегрирован в подсистему безопасности Windows NT/2000/XP/2003. PortsLock позволяет контролировать использование пользователями TCP/IP-протоколов на локальном компьютере. Контроль доступа к портам и IP-адресам осуществляется подобно контролю доступа к файлам и директориям на NTFS-разделе жесткого диска. Возможна установка разрешений в зависимости от времени и дня недели.

Ashampoo Firewall

(http://www.ashampoo.com)

Если у вас по каким-либо причинам не лежит душа к продуктам ZoneAlarm, рекомендую вам «двойника» этой линейки от Ashampoo. Версия Free – фейрволл в чистом виде, с минимумом дополнительных возможностей (исключая разве что фильтрацию спама по IP, встроенный Process Manager и «чистилку»). Возможно, и не самый надежный, однако по своим способностям он в любом случае превосходит стандартный брандмауэр Windows (который лучше всего сразу же отключить). По принципу работы напоминает тот же ZoneAlarm или Outpost: у программы два ре-

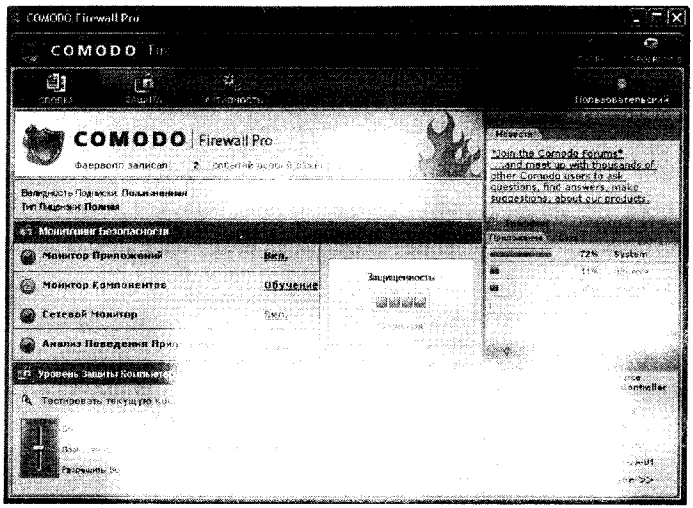
Ashampoo Firewall

жима – стандартный и «обучаемый» плюс кнопка блокировки всего трафика. В любом случае, бесплатных программ такого класса, увы, немного. Платная версия Pro умеет бороться с вирусами и троянами, блокировать рекламу... Однако, на мой взгляд, куда удобнее использовать бесплатную версию в связке с хорошим антивирусом типа NOD 32: Ashampoo никогда не славилась собственными антивирусными разработками.

Comodo Firewall

(http://www.personalfirewall.comodo.com)

Эта программа появилась на рынке всего около года назад, и поначалу особого внимания



Comodo Firewall

на нее не обратили. Еще бы: к тому времени на рынке уже было представлено несколько десятков аналогичных программ, да и поговаривали, что нужда в «брандмауэрах» чуть ли не окончательно отпадет после выхода Defender и LiveCare от Microsoft... Однако со временем многие конкуренты Comodo (Tiny, Kerio и так далее) либо сошли со сцены, либо превратились в обычные коммерческие продукты. Comodo же остался не только полностью бесплатным «брандмауэром», но и одним из немногих, поддерживающих русскоязычный интерфейс! А это позволяет ему соперничать даже с такими платными продуктами, как Outpost (от которого, кстати, Comodo не сильно отстает по количеству настроек). Интерфейс программы значитель-

но удобнее, чем у ZoneAlarm или Outpost, но не грешит и излишней простотой, как в Norton Internet Security. Поддерживается работа с несколькими «Зонами» (Интернет, локальная сеть), для каждой из которых можно создать свои правила, как и для отдельных приложений. Есть фильтр по IP-адресам. Разумеется, в программе нет антивирусных модулей, да и по части Spyware Comodo не силен... Зато как фейрволл он, вне всякого сомнения, входит в первую пятерку программ, которые я спокойно могу порекомендовать любому пользователю.

Анонимный серфинг и приватность

Не меньше атак и других пакостей в наш адрес раздражает ... пристальное наблюдение за нашими действиями: какой сайт мы посетили, на какие кнопки клавиатуры нажали и т. д. Неустанное и неусыпное. Не прерывающееся ни на секунду...

Ученые говорят, что отсутствие хоть толики уединения, приватности способно свести человека с ума в самые короткие сроки. Вспомним страдания героя Джима Керри в фильме «Шоу Трумена» – а ведь с парнем-то и не делали ничего

страшного, не пытали и «Маски-шоу» на дому не устраивали. Просто – наблюдали...

Время от времени возникает в сознании навязчивый вопрос: «А не контролируют ли мои путешествия по Сети?» Неважно кто – начальство, коллеги по работе или любимые всеми фибрами тела домашние. Неважно, по какой причине – начальству или службе безопасности на работе это по должности положено, и в большинстве западных компаний такая слежка в порядке вещей. Неважно и то, что ничего противозаконного вы можете и не делать – по неприличным сайтам не шатаетесь, наркотиками в Сети не торгуете...

Дело в том, что у проблемы конфиденциальности во Всемирной Паутине существует и еще одна сторона. Даже если вам совершенно безразлично, следят или нет за вашими перемещениями домашние, вам наверняка страшно не хочется, чтобы вас «посчитал» какой-либо из посещенных вами серверов. Мало ли что... Известно ведь, что любой зашедший на страничку пользователь неизбежно оставляет «следы»: IP-адрес его компьютера фиксируется в журнале-«логе» сервера.

А ведь IP-адрес может привести любого желающего прямехонько к вашему реальному, домашнему адресу или телефону...

И дело не только в этом. Честному пользователю бояться нечего – фиксируйте на здоровье! Однако существуют сайты, маскировочным способностям которых позавидуют и хамелеоны: каждому своему гостю они представляют совершенно различную информацию, в зависимости от того, из каких краев тот пожаловал. Частенько этот сервис удобен, но иногда серьезно раздражает. Другие сайты и вовсе не настроены раскрывать свою душу перед посторонними – американцев, к примеру, ждут с распростертыми объятиями, а перед жителями других стран опускают виртуальный шлагбаум. В лучшем случае – интеллигентно выталкивают в шею на свое региональное отделение.

Для преодоления этой напасти можно прибегнуть к услугам «веб-маскировщиков» (anonymizer) или столь же анонимных прокси-серверов.

Hide IP Platinum

(http://www.recuva.com)

Одна из самых простых и популярных программ для обеспечения приватности в Сети. Hide IP позволяет вам оставаться анонимными, подменяя Ваш реальный IP-адрес на адрес анонимного прокси-сервера. С настройкой программы абсолютно никаких сложностей не возникнет —

просто запустите ее, а Hide IP сама будет искать нужные сервера и при необходимости переключаться с одного на другой. Программа имеет модуль удаления (гарантированно невосстановимого) с жесткого диска, одним нажатием на кнопку, любого файла и следов пребывания в Интернете. Так же Hide IP содержит в себе средства для блокирования всплывающей рекламы и ActiveX и JavaScript. Русского интерфейса у программы нет, однако на сайте MSI Lab можно всегда скачать специальный русификатор для последней версии.

Hider IP

(http://allanonymity.com)

IP Hider — программа для обеспечения анонимности в интернете и сокрытия следов вашей деятельности в нем, в отличие от Hide IP, имеется возможность выбрать из списка IP страну/адрес на ваше усмотрение, затем протестить выбранный IP на работоспособность (время отклика, скорость и т.п.). Кроме периодической смены IP, программа умеет по заданному вами расписанию очищать журнал браузера, временные файлы, списки адресов и сохраненные пароли. Имеется возможность блокировки JAVA апплетов и элементов ActiveX. Возможно как ручное добавление списков прокси, так и онлайновое их обновление.

Don't Panic! privacy software

(http://www.panicware.com/product_dp.html)

Программа для страдающих паранойей:) Позволяет очистить на компьютере практически все следы вашей работы – кеш браузера, список последних документов (включая медиаплеер), очистить диск, и т. д., и т. п. ...

IE Security Pilot

(http://colorpilot.ru/iesecuritypilot/)

Информация автора:

IE Security Pilot поможет вам уничтожить следы путешествий по сайтам в Интернете. Просто кликните на иконку программы в трее (где часы), включите программу и просматривайте любые сайты. Для завершения безопасного просмотра – просто кликните иконку программы снова и IE Security Pilot уничтожит все следы просмотра интернет-страниц (кеш, куки и историю) без возможности восстановления с помощью спец. программ, таких как «unerase» и многих других.

Ключевые возможности:

3 режима безопасности:

Нормальный (normal) – основан на обычном сравнении файлов.

Высокий (high) – основан на детальном сравнении файлов (включая атрибуты файлов).

Высочайший (highest) – основан на вычислении дайджеста для каждого файла плюс все предыдущие режимы.

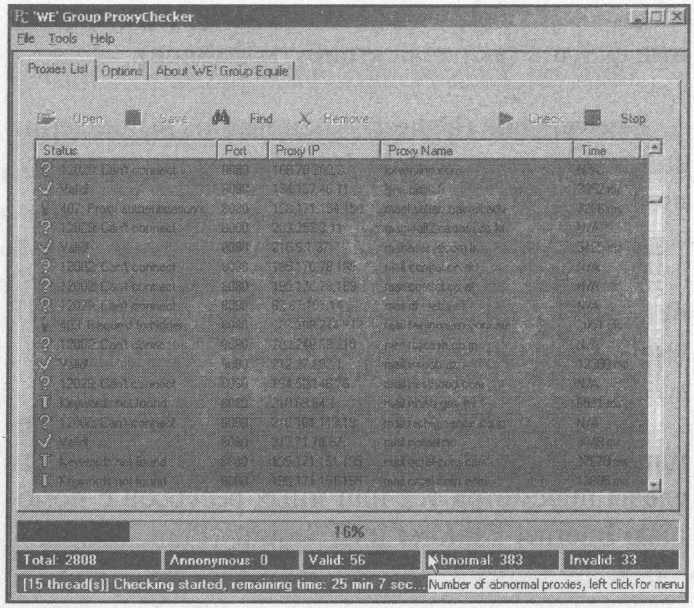
Возможность уничтожения следов путешествий по Интернету в кеше, cookies и истории IE вместо обычного удаления файлов.

Итак, вы можете быть уверены, что даже специалист не сможет никаким образом обнаружить следы просмотра тех или иных ресурсов с помощью Internet Explorer и IE Security Pilot.

ProxyChecker

(http://www.wegroup.org/proxychecker/)

Прокси-сервером именуется компьютер, через который и происходит наше с вами общение с Сетью – именно через него отправляются все наши запросы на получение информации со страничек или файлов. Прокси не просто служит «воротами» в Интернет и «копилкой» для проходящей через него информации: он может защищать ваш компьютер от вредоносных программ или не слишком желательной (с точки зрения провайдера) информации.



ProxyChecker

Как правило, адрес прокси-сервера из собственных запасов предоставляет вам провайдер. Однако в некоторых случаях бывает полезно заменить ваш стандартный прокси-сервер на другой – анонимный. И главное – общедоступный.

К великому сожалению пользователей, стандартные прокси-серверы обладают некоторыми задатками порядочности – обращаясь по просьбе пользователя к удаленному компьютеру, они сообщают последнему не только свой собственный сетевой адрес, но и IP-адрес пользователя-

«заказчика». Разумеется, последнего в итоге не слишком трудно вычислить... Не стоит думать, что теперь хозяин любого посещенного вами сервера может узнать ваше имя, домашний адрес, а заодно и номер счета в банке – такие детали интересуют не слишком многих. Однако и информацию более общего плана (из какой страны «пришел» пользователь, через какого провайдера подключился) в некоторых случаях уместно скрыть, если уж вы так озабочены проблемами анонимности. В этом вам и помогут «анонимные» прокси, которые свой адрес сообщают с удовольствием, а ваш, пользовательский – нет.

Программа ProxyChecker предназначена для проверки списка прокси-серверов на анонимность. Имеет очень удобный и простой интерфейс. Позволяет указать число потоков для проверки списка, тем самым позволяя подстроиться под свою линию. Вы можете легко манипулировать списком прокси-серверов: записывать раздельно хорошие и плохие, удалять, записывать весь список.

SocksChain

(http://www.apssoft.com)

SocksChain – программа, позволяющая работать через цепочку SOCKS или HTTP прокси, для того чтобы скрыть истинный IP-адрес.

SocksChain может работать как обычный SOCKS-сервер, транслируя запросы по цепочке прокси-серверов. SocksChain может быть использован с клиентскими программами, которые не поддерживают протокол SOCKS, но работают с одним TCP-соединением, например TELNET, HTTP, IRC... При этом ваш IP-адрес не будет появляться в логах сервера или заголовках почтовых сообщений.

Shadow Professional

(http://www.systenance.com)

Вряд ли даже самый отъявленный параноик думает о приватности постоянно. Скорее – время от времени, в момент посещения каких-либо сайтов, которые по каким-либо причинам нежелательно являть на глаза посторонним. Обычные меры, вроде очистки Журнала и сохраненных форм, кажутся слишком хлопотными в таких случаях. Вот если бы можно было становиться «невидимкой» на время, без всякой возни с настройками...

С уже упоминавшейся программой Shadow Professional это не составит никакого труда. Достаточно лишь нажать на кнопку Start – и вы тут же переходите в «теневой» режим: история ваших путешествий в Журнале браузера не фиксируется и никаких следов на компьютере не остается. Впрочем, это далеко не все: с помощью

«тени» можно создавать на компьютере папки и файлы-невидимки – например, секретный раздел в вашей папке «Избранное», зайти в который сможете только вы. Кроме того, «тень» может поработать и неплохим чистильщиком, тщательно удалив историю браузера и прочие следы ваших сетевых странствий.

Средства шифрования

PGP Desktop

(http://www.pgp.com)

PGP (Pretty Good Privacy) — лучшая программа шифрования данных для настольных систем, созданная Филиппом Циммерманом еще в 1991 году! PGP уже давно признана фактическим стандартом стойкого шифрования в Интернет. Она позволяет надежно защитить от прочтения как вашу электронную почту, пока она находится на пути к адресату, так и файлы, хранящиеся на любом носителе. Даже если вы не герой-разведчик, передающий в Центр сверхсекретную информацию, а простой человек, не желающий, чтобы его личная информация стала достоянием третьих лиц, — эта программа для вас.

Ее работа основана на принципах криптографии с открытым ключом: вам не будет нужды вместе с файлом или письмом передавать к нему пароль. Все, что нужно, это сгенерировать пару ключей и опубликовать один из них — открытый — в Интернете, откуда его сможет получить каждый. Этот ключ позволит любому человеку (даже тому, с кем вы прежде никогда не общались) зашифровать для вас послание, которое только вы сможете прочитать благодаря второму ключу из пары — закрытому, хранящемуся только у вас. На первый взгляд это может показаться сложным, но на самом деле все очень просто.

Pgp Desktop состоит из нескольких модулей каждый из которых ориентирован на определенную задачу:

PGPmail — защита почтовых отправлений,

PGPdisk — создание виртуального шифрованного диска (аналог BestCrypt),

PGPicq — Этот модуль для популярной программы ICQ позволяет шифровать вашу переписку, ведущуюся с помощью данной программы. Хорошая штучка для любителей посекретничать...

SecureFX

(http://www.vandyke.com)

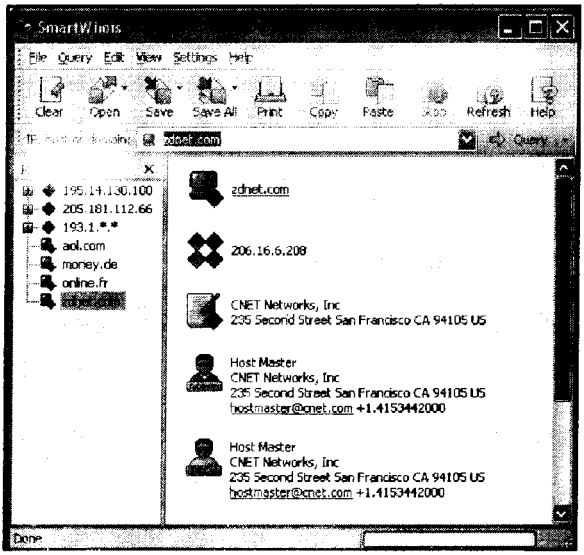
Клиент для зашифрованной передачи файлов с широкими возможностями настройки конфигурации и протоколов передачи. SecureFX включа-

ет в себя утилиту для осуществления передачи файлов по протоколу SSH из командной строки. SecureFX также поддерживает режим докачки и восстановления связи в случае ее обрыва.

Информационные утилиты

SmartWhois

(http://www.tamos.com/products/smartwhois/)



SmartWhois

SmartWhois – удобное средство получения информации о любом IP-адресе или имени компьютера в мире. В отличие от стандартных whois-утилит SmartWhois автоматически находит информацию об IP-адресе независимо от того, где этот адрес зарегистрирован географически. Всего лишь за несколько секунд вы можете узнать все что хотите о пользователе: домен, сетевое имя, страну, штат или провинцию, название города. Даже если данному адресу не сопоставлено имя, SmartWhois все равно выполнит свою работу.

Ping Plotter

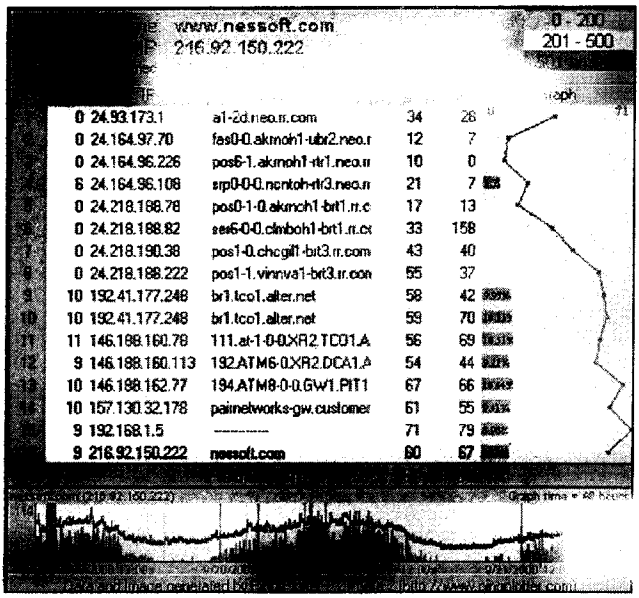
(http://www.pingplotter.com)

Очень приятный графический traceroute. Помимо хостов, через которые проходят пакеты, строит график задержек и мониторит скорость соединения с сервером... Запускает несколько процессов, благодаря чему результаты появляются быстрее, чем при использовании обычного traceroute.

WinDump

(http://netgroup-serv.polito.it/windump/)

Все, кто работал с Юниксом и сетями, наверняка знают такую полезную утилиту, как TCPdump. Теперь она есть и под Windows... С помощью этой утилиты вы сможете отслеживать все



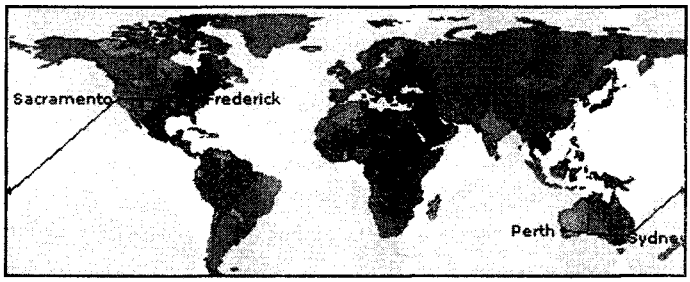
Ping Plotter

взаимодействие вашего компьютера с сетью, что весьма полезно при вычислении различных проблем, а иногда и просто интересно... До того, как запускать саму программу, вам надо установить соответствующий пакетный драйвер (это делается в настройке сети в панели управления, драйвер ставится как протокол).

VisualRoute

(http://www.visualroute.com)

Программа, напоминающая те, что показывают в фильмах про хакеров. Это traceroute, кото-



VisualRoute

рый показывает на карте мира расположение роутеров, через которые проходят пакеты. Естественно, только те, о которых она знает или может догадаться. Помимо traceroute есть также Whois. Для работы программы требуется, чтобы у вас была установленна Java VM (если у вас стоит IE 4.01+, то у вас она уже есть).

Whois, Finger, and Host Utilities

(http://www.kiraly.com)

Консольные версии этих полезных сетевых утилит, работающие под Windows... Их очень удобно положить в какую-нибудь папку, прописанную в переменной PATH, а затем вызывать из, например, FAR manager-a...

Мониторы

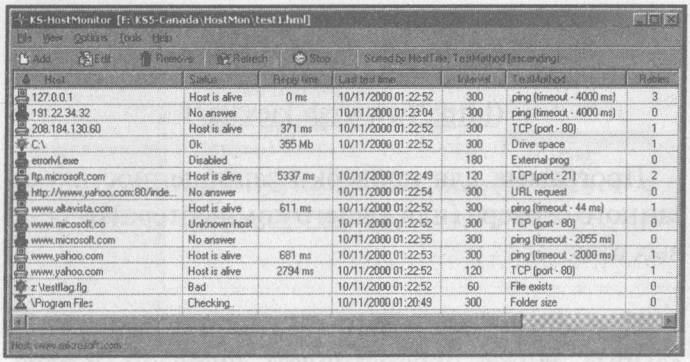
HostMonitor

(http://www.ks-soft.net/hostmon.eng/index.htm)

Монитор сетевых ресурсов. Умеет контролировать доступность физических устройств (Ping тест), работоспособность TCP сервисов (например WWW, FTP сервера), доступность страниц через HTTP, HTTPS протоколы.

Может также контролировать локальные ресурсы (объем свободного дискового пространства, размер каталогов или файлов), и т. д., и т. п.

При изменении статуса устройства монитор может выполнить набор заданных действий: выдать звуковое или визуальное предупреждение, послать e-mail (например на пейджер или сото-



HostMonitor

вый администратору сети), сформировать HTML отчет, запустить внешнюю програму, перегрузить компьютер и т. д.

Для разных заданий можно определить разные расписания (когда вести контроль), разные наборы действий при изменении статуса.

Монитор умеет вести лог в HTML, DBF и текстовом форматах с различной степенью детализации.

Имеет встроенный viewer и анализатор log-файлов.

Цена программы зависит от количества задач, которые надо отслеживать.

Сканеры

ShadowSecurityScaner

(http://www.rsh.kiev.ua/)

Программа для проверки защищенности указанного сервера (или вашего компьютера) от сетевых атак.

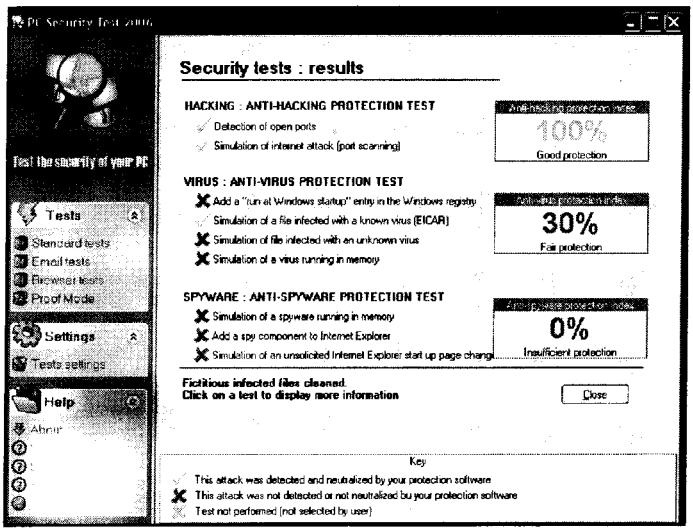
Проверяет открытые порты и стандартные «дыры». Может просматривать диапазон IP-адресов. Заодно рассказывает, чем именно опасна та

или иная «дыра»... Удобный интерфейс, толковые настройки, полезные отчеты... Очень хороший инструмент для сисадмина!

PC Security Test

(http://www.pc-st.com)

Бесплатная программа для проверки защиты вашего компьютера. PC Security Test имитирует хакерскую атаку, проникновение на компьютер известного или неопознанного вируса, рекламных и хакерских модулей. Всего в программу входит около десятка тестов. Можно ли доверять этой утилите? Целиком и полностью вряд ли, по-



PC Security Test

скольку на моем компьютере, защищенным с помощью стандартного брандмауэра Windows XP, тест показал стопроцентную защищенность от хакерских вторжений. А антивирусная защита, которую обеспечивал маститый антивирус NOD 32, была оценена лишь в 30 % от необходимого уровня (здесь разработчики явно рекламируют собственный антивирус VirusKeeper)! Однако результаты PC Security Test всех же показательны и способны моментально сбить спесь с тех, кто считает свой компьютер абсолютно неуязвимым.

PC Super Scanner

(http://www.pcinternetpatrol.com)

Кроха-сканнер, способный за несколько секунд проверить ваш компьютер на уязвимость. Программа выдает вам список открытых портов и порекомендует средства для устранения брешей в защите. На сайте разработчика вы сможете найти подробную документацию по различным портам с указанием степени потенциальной опасности каждого из них.

CommView

(http://www.tamos.com/products/commview/)

CommView является инструментом для мониторинга сетевой активности с возможностью записи и анализа пакетов в сетях типа Ethernet.

Программа способна собирать информацию о данных, передаваемых в локальной сети, декодировать и анализировать их. При помощи CommView вы можете наблюдать за сетевыми соединениями, ключевой статистикой протокола IP, а также просматривать содержимое отдельных пакетов. Пакеты IP декодируются до самого низкого уровня с возможностью полного анализа основных протоколов IP: TCP, UDP, и ICMP. Есть также функции полного доступа к необработанным данным.

Программы для борьбы со спамом

За все удобства рано или поздно приходится платить! Этот закон – один из двух Великих, Вечных и Нерушимых устоев, на которых держится Вселенная. Второй, как можно легко догадаться – это известный всем и каждому Закон Подлости или Оборотной Стороны, как кому удобнее. Словом – у каждой «халявы» всегда есть оборотная сторона, которая то и дело норовит испортить все удовольствие от использования свалившегося из ниоткуда подарочка.

За удобство, доступность и практическую бесплатность электронной почты, равно как и за пользование другими «бесплатными» ресурсами

Интернета, вам неизбежно придется платить, тратя огромные усилия на борьбу с рекламными письмами, которые будут каждый день сваливаться в ваш почтовый ящик. Откуда, каким образом? И вы еще спрашиваете... Разве не вы заполняли небольшую форму на сайте, предоставляющем вам какие-то бесплатные услуги – тот же почтовый ящик? А внимательно ли вы прочитали перед этим пользовательское соглашение? Вот то-то и оно.

Разумеется, далеко не все владельцы бесплатных «почтовиков» устраивают своим посетителям такую подлянку. Но ведь не только в них дело! «Бесплатных» мышеловок, напичканных «сыром» стопроцентного качества, в Сети достаточно. И задача многих из них – заполучить ваш почтовый адрес, дабы завалить вас горами обещаний, предложений, опросов... Хорошо, если это будет одно-два сообщения в день... А если больше?

Надоедливые рекламные письма, переполняющие наши почтовые ящики, стали едва ли не самой главной напастью наших дней. Аналитики подсчитали: количество «спамовых» писем сегодня составляет почти половину(!) от всех получаемых нами сообщений.

Забавно, что свое название почтовый мусор унаследовал... от обычных мясных консервов компании Hormel Foods, выпускавшихся в США еще с 20-х годов прошлого столетия! Низкая стоимость этой тушенки из свиных ножек сдела-

ла ее самым популярным блюдом на столах обедневшего во время кризиса «среднего класса», а позднее, во время Второй мировой войны – основным блюдом в рационе солдат союзнических армий.

В послевоенные годы компании пришлось «стимулировать» спрос с помощь крикливой рекламы: «спам» царил везде – на страницах газет, на экранах телевизоров, не говоря уже о специализированных кулинарных книгах, посвященных блюдам из тушенки!

Кульминацией «спамовой лихорадки» стало комическое шоу знаменитой английской группы «Monty Piton Flying Circus», с триумфом прошедшее по телеэкранам Америки в начале 70-х годов – все его действие происходило в «спамовом» ресторане, и слово «спам» звучало с экрана чуть ли не каждую секунду. Официантки разносили по столикам блюда, изготовленные исключительно из спама, а с эстрады звучала вдохновенная ода чудо-консервам в исполнении хора викингов...

Понятие же «почтового спама» появилось на свет благодаря активной деятельности супружеской четы американских адвокатов – Лоренса Кантера и Марты Сигел. В начале 1978 года их компания буквально потопила немногочисленных тогда пользователей Сети в массе рекламных писем...

Увы, никакой коммерческой выгоды (кроме разве что сомнительной славы) первооткрыватели «спама» так и не обрели: возмущенные адресаты их писем добились того, что оба первых «спамера» были лишены адвокатской лицензии, а их компания была закрыта. Впрочем, это не помешало Кантеру и Сигел в дальнейшем зарабатывать на жизнь написанием руководств на тему «Как правильно рекламировать ваш бизнес в Интернете»...

Зато преуспевают их последователи – по оценке исследователей, в 2003 году профессиональные компании-«спамеры» разослали по Сети рекламных сообщений почти на миллиард долларов!

Поначалу эпидемия «спама» поразила группы электронных новостей, а вскоре «зараженными» оказались и личные почтовые ящики пользователей. И сегодня в Америке существует несколько фирм, специализирующихся на рассылке электронной рекламы по личным адресам пользователей. Чтобы попасть в список к «спамерам», иногда достаточно всего один раз «засветить» свой адрес, например, в одной из групп новостей.

Прибегают спамеры и к хитростям. Например, если к вам приходит электронное письмо с рекламой какой-либо услуги и предложением в случае вашего отказа написать по указанному в письме адресу, девяносто девять шансов из ста, что это – работа спамера. Ответьте на такое

письмо вежливым отказом, и спамер поймет, что адрес работает и хозяин его почту читает. И уж тогда – держитесь!

Частично избавить себя от спама можно благодаря использованию нескольких почтовых ящиков. Один адрес используйте только для приватной переписки, не засвечивая его в Сети, и выдавая лишь самым доверенным людям. Для писем в группы новостей, гостевые книги и т. д. используйте второй ящик. Наконец, третий адрес указывайте при регистрации на различных сайтах – вам изначально будет понятно, что кроме мусора там ничего ценного быть не может.

Хотя даже после этого надеяться на то, что ваш почтовый ящик будет защищен от этой зудящей и надоедливой сетевой «мошкары», было бы с вашей стороны просто наивно! Однако не стоит паниковать, обнаружив в почтовом ящике первое рекламное сообщение. Спокойно жмите на кнопку ***Del*** и переходите к следующему сообщению. Особо надоедливых «спамеров» можно отлучить от вашего почтового ящика с помощью механизма фильтрации Outlook Express.

Отфильтровать спам поможет уже хорошо знакомая нам система сортировки.

Переведите курсор на полученное «мусорное письмо», щелкнув по его заголовку левой кноп-

кой мышки. Теперь укажите курсором на пункт ***Сообщение*** текстового меню вверху экрана Outlook Express, активируйте его щелчком, и выберите пункт ***Создать правило из сообщения***.

Вы увидите уже хорошо знакомый нам бланк сортировщика, в поле ***От:*** которого внесен адрес отправителя «спама». И теперь нам остается только пункт ***Удалить с сервера*** в разделе ***Действия*** (для перехода в конец списка действий воспользуйтесь «бегунком» в правой части окна бланка). Ура! – письма от этого адресата больше не будут загружаться на ваш компьютер, а будут зверски убиты прямо в почтовом ящике. Учтите только, что хитрые спамеры постоянно меняют адреса – значит, нам придется повторять эту процедуру снова и снова.

В «черный список» кандидатов на уничтожение можно занести не только адреса электронной почты, но и письма с определенными словами в поле ***Тема*** – но с этим, как я полагаю, вы справитесь уже самостоятельно. Поработав с электронной почтой неделю-другую, вы сможете составить свой список слов, которые чаще всего встречаются в заголовках «спамовых» писем. К их числу можно отнести, например, такие: Sex, Free, Viagra, Penis, Vacations, Gift, XXX... и так далее.

Конечно, простое наличие любого из этих слов в заголовке письма еще не говорит о том, что это письмо – стопроцентный спам. Но ве-

роятность такая есть, и довольно большая. Правда, если вы большой любитель крутить виртуальные романы с зарубежными дамами/джентльменами, такие письма удалять не стоит. Если же нет... Словом, решайте сами. В крайнем случае, письма с «опасными» заголовками можно не удалять, а просто отправлять в специальную папку – для дальнейшего, более пристального изучения.

Кардинальным инструментом для борьбы с «почтовым хламом» является пункт ***Блокировать отправителя*** того же меню ***Сообщение***. Его активация не только поставит заслон на пути последующих писем от выбранного вами адресата, но и очистит компьютер от всех принятых ранее писем с этого адреса.

Но и этого мало – многие рекламные письма приходят с «разового» адреса, который буквально на следующий день меняется спамером на другой. Тут фильтры уже не помогут... Но зато может помочь отличная программа под названием MailWasher (http://www.mailwasher.net).

Kaspersky Anti-Spam

(http://www.kaspersky.ru)

Первая профессиональная программа для борьбы со спамом, созданная в России.

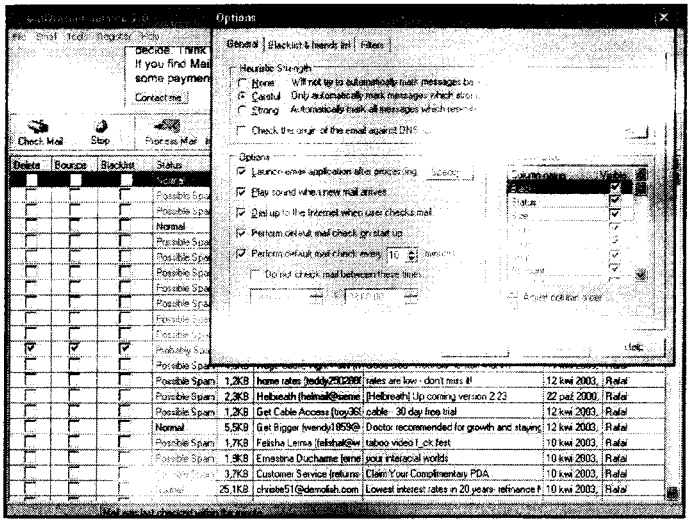
Kaspersky Anti-Spam является высокоинтеллектуальной системой защиты от спама, предназначенной для предприятий с сетями малого и среднего масштабов. Данное решение – результат совместной разработки специалистов «Лаборатории Касперского» и компании «Ашманов и партнеры».

Эффективность решения обеспечивается за счет одновременного использования системы обновляемых в режиме on-line «черных» списков, использования образцов писем и применения мощной системы эвристического анализа (интеллектуального смыслового анализа) входящей корреспонденции. Программа обеспечивает фильтрацию почтовых сообщений еще до их попадания в ящики конечных пользователей. Таким образом, использование продукта позволит значительно сократить затраты на обслуживание почтовой системы, а также непроизводственные затраты рабочего времени сотрудников.

MailWasher

(http://www.mailwasher.net)

Занесите в программку адреса ваших почтовых ящиков и все необходимые сведения для доступа к ним. А затем, подключившись к Интернету, нажмите кнопку Check Mail: программа проверит ящики и вытянет заголовки всех писем. А уж за-



MailWasher

тем вы можете с ее помощью удалить ненужные письма с сервера, даже не загружая их. В сомнительных случаях можно затребовать и текст письма, а уж затем окончательно решить его участь. В дальнейшем программа поселится в вашей «области задач» в правом нижнем углу экрана и периодически будет проверять ваш почтовый ящик – нет ли новых писем? При наличии «новичков» программа оповестит вас об этом и продемонстрирует заголовки вновь пришедших сообщений.

Правда, такой фокус может проделывать громадное количество других программ – та же ICQ, например. А в почтовую программу The Bat! такая утилита и вовсе встроена изначально... Но не то-

ропитесь – ведь мы еще изучили не все возможности MailWasher.

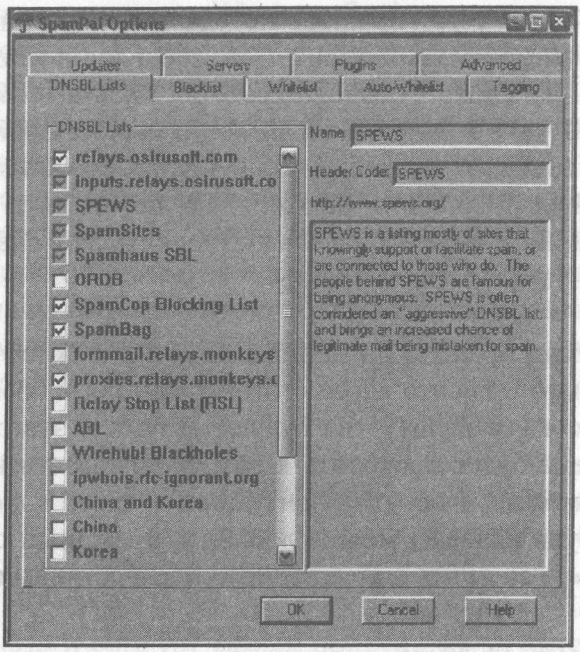
Помимо ручной фильтрации сообщений существует и автоматический режим – подобно почтовой программе, MailWasher снабжен собственной системой фильтрации. При этом в «черный список» программы уже внесено несколько сотен адресов самых известных поставщиков «спама». Это не так уж много, но какую-то часть мусора программа сумеет отсечь даже без дополнительной настройки.

С помощью опции Bounce Mail вы можете отправить на адрес спамера фальшивое сообщение о «смерти» вашего почтового ящика – мол, не найден адресат! Некоторые спам-программы на такие сообщения реагируют, исключая ваш ящик из списка рассылки. Правда, такой прием бесполезен против писем с фиктивными обратными адресами – ваш «отлуп» просто не дойдет до настоящих отправителей, так что его эффективность вызывает сегодня большие сомнения.

SpamPal

(http://www.spampal.org)

Другой удачной программой для борьбы со спамом является бесплатная (на данный момент) утилита SpamPal. Эта программа гораздо более гибка в области настроек – к примеру, вы можете задать выборочную проверку почтовых ящиков,



SpamPal

блокировать почту из определенных регионов мира. «Спамерская» база данных SpamPal поражает своим объемом и регулярно обновляется – вам остается лишь периодически запрашивать сайт программы на предмет новых дополнений.

Единственным недостатком этой программы является необходимость ручной настройки – принцип «установи и работай» здесь явно остается в стороне. Настройки для работы SpamPal в связке с Outlook Express вы можете найти здесь:

http://www.spampal.org/usermanual/oe/oe.html

Кроме того, SpamPal не удаляет «мусорные» письма, а только помечает их, добавляя в заголовок каждого сомнительного письма слово ***SPAM***. Зато потом вы легко можете отфильтровать их с помощью стандартных механизмов Outlook Express – рекомендую не удалять все письма скопом, а сначала копировать их в специальную «мусорную» папку.

Если SpamPal по ошибке пометил нужное вам письмо, внесите адрес его отправителя в «белый список» (whitelist) – и в будущем почта от этого человека будет проходить к вам беспрепятственно. Возможна и обратная ситуация – адрес какого-нибудь надоеды можно добавить в «черный список» – со всеми вытекающими последствиями.

Средства шифрования и управления доступом

Ashampoo Magical Securiy

(http://www.ashampoo.com)

Программа для защиты конфиденциальных данных любого типа — файлов, личных писем, приватных картинок, служебных данных и т. п., находящихся на жестком диске, CD или DVD.

Интегрируется с Windows Explorer, так что процесс шифровки/расшифровки (поддерживается стойкий к взлому алгоритм AES) может производиться очень быстро и легко — в один клик. Дополнительные возможности: гарантированное — без возможности восстановления — удаление данных, шифрование данных одновременно с их записью на CD или DVD, интеграция с почтовым клиентом, создание зашифрованных самоизвлекающихся архивов. Есть русскоязычный интерфейс.

DriveCrypt

(http://www.drivecrypt.com)

Это и есть тот самый продукт, из-за которого прекратилась поддержка Scramdisk-а. Продукт действительно вышел более чем удачным – он перенял все лучшее, что было в Скрамдиске, включая основную функциональность, и добавил несколько новых приятных свойств. Во-первых, файлы, в которых хранятся зашифрованные данные, не имеют каких-либо специфичных заголовков, так что в случае возникновения каких-то сложностей практически невозможно доказать, что тот большой файл на диске на самом деле является виртуальным контейнером. Во-вторых, в программу встроена улучшенная защита от взлома – время проверки пароля после каждой неудачной попытки увеличивается, что

помогает защититься от попыток взлома по словарю. Кроме того, встроена защита от кражи пароля «троянцами» или чем-то подобным. В-третьих, появилась возможность многопользовательской работы – при установке программы создается администраторский пароль, а администратор может выдавать пароли с более низким приоритетом пользователям. Причем эти пароли могут быть ограничены по времени. В-четвертых, в программу встроен скринсейвер, запирающий компьютер, если он на какое-то время был оставлен без присмотра. В-пятых, программа умеет «качественно» удалять данные с диска. В-шестых... В-седьмых... В общем, много всяких «вкусностей» добавилось...

Steganos Security Suite

(http://www.steganos.com/en/)

Эта программа «выродилась» из сравнительно простой шифровалки в целый программный комплекс, обеспечивающий безопасность ваших данных. Изначально Steganos получил признательность во всем мире за умение «прятать» зашифрованные данные внутри других «невинных» файлов, например, картинок или звуковых файлов. То есть вы могли написать сообщение, «вложить» его, скажем, в картинку и по открытой электронной почте отправить своему коллеге. А тот, зная пароль, мог без проблем «из-

влечь» ваше сообщение из полученной картинки.

Эта способность осталась и сейчас, но к ней добавились системы надежного удаления информации с винчестера, «запирание» компьютера от любопытных коллег, шифрование электронной почты, утилита для хранения паролей, виртуальные диски, все данные на которых автоматически шифруются и многое другое. Словом – «мой компьютер – моя крепость»...

Private disk

(http://www.dekart.com/products/encryption/private_disk/)

Private disk позволяет создавать образы дисков на локальных и сменных носителях и работать с ними стандартным образом. Виртуальный зашифрованный диск представляет собой обычный файл — так называемый *файл-образ диска*, в котором данные хранятся в зашифрованном виде. После подключения файла-образа с помощью Private disk операционная система определяет его, как обычный диск, назначая ему соответствующую букву. Если в Вашей системе имелись жесткие диски, определяемые буквами C: и B:, то после активации шифрованного диска появится, например, буква E:. Файл-образ виртуального зашифрованного диска может

иметь любое имя, расширение и путь доступа к нему (даже сетевой).

Кроме того, программа может работать на съемном диске. Минимальный размер виртуального зашифрованного диска 1 MB, максимальный: 2.1 GB (Windows 95 , Windows 98 , Windows ME) и 1 TB (Windows NT, Windows 2000, Windows XP, Windows 2003).

Подключение зашифрованного диска и работа с зашифрованными данными возможны только при предъявлении пароля.

Зашифровать конфиденциальную информацию тоже очень просто — надо лишь перенести ее со старых носителей на новый зашифрованный диск и не забывать впоследствии сохранять конфиденциальную информацию именно на него, а открытую информацию — на любые другие диски. В качестве алгоритма шифрования виртуального диска используется американский стандарт Advanced Encryption Standard (AES) в режиме ***CBC*** с длиной ключа шифрования *256* бит. *Надежен ли такой* ключ *шифрования?* Да! По оценке Брюса Шнайера *(Bruce Schneier, Applied Cryptography)* даже для подбора ключа шифрования длиной 123 бит необходимо наличие 4,2×1 022 процессоров производительностью *256* миллионов операций шифрования в секунду. Но даже в этом случае ключ будет взломан только через 1 год. В качестве

генератора случайных последовательностей применяется криптографическая функция хеширования SHA-1.

В связи с этим интересно упомянуть, что Dekart Private Disk позволяет восстановить забытый пароль доступа к виртуальному зашифрованному диску методом полного перебора (Brute-force). Например, пароль из 5 цифр мой компьютер (при указании в параметрах перебора только цифр) определил за 15 секунд.

Данная возможность нисколько не снижает уровень безопасности зашифрованных данных при условии выбора криптографически сильного пароля.

Hide Folders XP

(http://www.fspro.net/)

С помощью этой небольшой программы вы сможете полностью скрыть от посторонних те папки, содержимое которых следует сохранить в секрете. Достаточно лишь запустить утилиту, выбрать необходимую папку и нажать кнопку «Hide», после чего папка будет доступна для чтения и записи только вами. При этом остальные пользователи не смогут увидеть ее — даже при установке «показывать скрытые папки». Снятие

грифа «скрыто от посторонних глаз» происходит точно таким же образом. Сама Hide Folders работает в скрытом режиме, поэтому невозможно определить, запущена она в данный момент или нет, то есть утилита может прятать себя сама и становиться полностью недоступной для просмотра чужаками.

- В программе доступно 3 режима защиты файлов и папок: скрывание, блокирование доступа и комбинированный (скрывание и блокирование доступа).
- Поддерживаются все основные файловые системы Microsoft Windows: NTFS, FAT32 и FAT.
- Hide Folders XP НЕ МОДИФИЦИРУЕТ структуру файловой системы, т. е. не может быть причиной сбоя в файловой системе или потери данных.
- Файлы в скрытых папках не будут потеряны даже тогда, если кто-нибудь попытается удалить папку уровнем выше.
- Удаление каталога программы не приводит к снятию защиты, файлы и папки будут по-прежнему защищены.
- Hide Folders XP позволяет скрывать неограниченное количество папок и файлов.
- Hide Folders XP позволяет установить пароль на запуск программы и на деинсталяцию программы.

- Hide Folders XP опционально позволяет скрывать файлы и папки в Режиме Защиты от Сбоев (safe mode).
- Поддерживаются имена файлов и папок, заданные национальными (нелатинскими) символами.
- Hide Folders XP имеет множество дополнительных полезных опций.

DeviceLock

(http://www.smartline.ru)

DeviceLock – это средство контроля доступа к сменным носителям и устройствам в системах, работающих под управлением Windows NT/2000/XP и Windows Server 2003. DeviceLock позволяет назначать права доступа для пользователей и групп пользователей, контролировать доступ к дисководам, CD-ROM-ам, принтерным и модемным портам и любым другим устройствам. При этом, поддерживаются все виды файловых систем – FAT, NTFS (версии 4 и 5), CDFS и т. п.

DeviceLock имеет встроенные средства удаленного администрирования, позволяющие контролировать доступ к устройствам на каждом компьютере в локальной сети.

Folder Lock

(http://www.newsoftwares.net/folderlock/)

Программа для ограничения доступа к выбранным вами файлам и папкам. Конечно, возможность защиты папок паролем реализована в Windows XP и Vista. Но штатные средства, как всегда, хотя и действенны, но не слишком удобны. Поэтому работенка для отдельных программ типа Folder Lock найдется всегда...

С помощью Folder Lock вы можете защитить выбранные файлы-папки паролем, закрыть к ним доступ, запретить вносить изменения – или вовсе спрятать их с глаз долой.

Вы можете спрятать не только отдельные файлы и папки, но и целые диски – достаточно запустить Folder Lock и отдать ему соответствующую команду. Для получения доступа к спрятанным данным достаточно запустить Folder Lock и ввести правильный пароль. Управление программой очень простое — поддерживается метод drag & drop (перетащил ▸ опустил ▸ спрятал). Еще одна (пусть и не самая важная) особенность программы — оригинальный нестандартный интерфейс.

TrueCrypt

(http://www.truecrypt.org)

Видели в голливудских фильмах сцены изъятия компьютера у злодеев-террористов-мафиози? Красавец ФБР-щик пытается залезть на жесткий диск, а тот в ответ лишь дразнит его окошком с требованием ввести пароль – иначе никакого доступа! В кино обычно такую защиту ломают за пару минут, в жизни все чуточку сложнее... Начнем с того, что программы шифрования дисков требуются не только голливудским злыдням, ими охотно пользуются и честные бизнесмены (если, конечно, такие в природе встречаются). А если этот бизнесмен еще и не обременен излишними деньгами, то он наверняка с благосклонностью отнесется к программе TrueCrypt – одной из немногих бесплатных систем шифрования, распространяемой по принципу Open Source.

Ключевые особенности:

- Создание виртуального зашифрованного диска внутри файла и монтирование его как настоящего диска.
- Шифрование как целых разделов жесткого диска, так и отдельных устройств (USB-брелоки с флэш-памятью, флоппи-диски и т. д.).

- Функция обманного ввода пароля.
- Алгоритмы шифрования: AES (256-бит ключ), Blowfish (448-бит ключ), CAST5 (128-бит ключ), Triple DES.
- Основана на алгоритме Encryption for the Masses (E4M) 2.02a.

Folder Guard

(http://www.winability.com/folderguard)

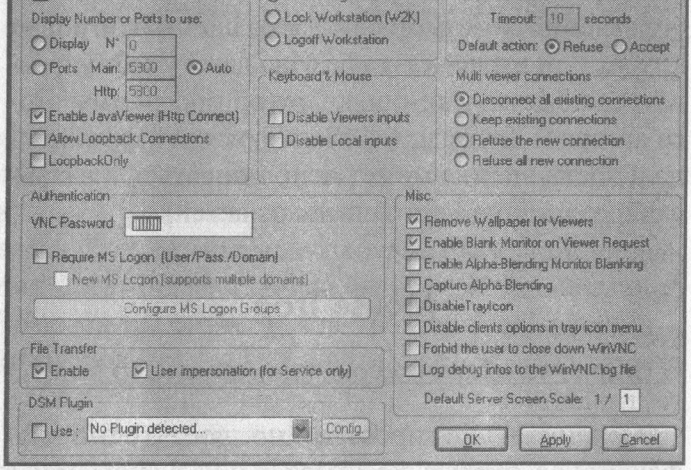
Эта программа занимается тем, что «прячет» определенные папки. Причем прячет их весьма качественно – они становятся невидимыми для любых приложений (в том числе консольных), запущенных из-под Windows. Программа просто перехватывает все обращения к файловой системе, и если запрос идет к «закрытой» папке или файлу, то отвечает, что такого нет... Разумеется, только если перед этим не был введен соответствующий пароль. Как и большинство других вещей, такой подход имеет как преимущества, так и недостатки. К преимуществам можно отнести надежность: даже если что-то произойдет с программой, ваши данные никуда не денутся, так как Folder Guard их никоим образом не модифицирует. Это же относится и к недостаткам – загрузившись в ДОС (например, с дискеты), все ваши данные можно будет прочитать... Но, несмотря на этот недостаток, программа может оказаться во многих случаях весьма полезной,

тем более, что помимо «маскировки» папок она умеет защищать файлы и папки от записи (не просто выставлять read-only атрибут!), запрещать пользователям устанавливать новые программы, запрещать запуск программ с дискет и много других мелких полезностей...

LockWin

(http://www.pisoft.ru)

Программа LockWin позволяет контролировать, как и сколько времени кто-либо другой использует ваш компьютер. Она загружается авто-



LockWin

матически при запуске Windows и помещает свой значок в Панель задач Windows (рядом с часами). Через этот значок, после ввода пароля, вы можете установить различные параметры доступа пользователей к компьютеру, в том числе и временной лимит. Когда этот лимит истечет, компьютер будет автоматически заблокирован. После запуска программы у пользователя нет возможности обойти эти ограничения, если он не знает пароля. Можно задать несколько временных интервалов доступа к компьютеру, установив в каждом интервале свои права на запуск разных групп программ (игры, интернет, офис, инструменты...). Программа ведет подробный отчет о работе компьютера, из которого можно узнать, какие и когда запускались программы, и многое другое.

В принципе, эта программа предназначена для управления компьютерами в различных игровых клубах или интернет-кафе (она даже умеет управляться по сети с помощью другой программы этого автора – Locker), но благодаря свой функциональности вполне может использоваться и в офисах и даже дома (для защиты от детей)...

Mouse Trap

(http://www.hotwww.com/ryan/mousetrap.html)

Сравнительно простая, но достаточно эффективная защита компьютера от сослуживцев или домашних. Занимается тем, что по вашей

команде (а можно и при старте компьютера или в определенное время) «запирает» мышку и одновременно блокирует сочетания клавиш ***Ctrl-Alt-Del***, ***Ctrl-Tab***, ***Alt-Tab***. Предусмотрено автоматическое восстановление после перезагрузки (если кто-то догадается нажать ***Reset***), умение автоматически «запирать» компьютер через сколько-то минут неактивности (наподобие скринсейвера), показ числа неудачных попыток ввести пароль... Есть также возможность автоматически освобождать мышку в заданное время.

Безвозвратное удаление информации

С каким трудом иногда приходится восстанавливать утерянную информацию! Легкое (и лишнее) движение руки, крохотный сбой – и нужный файл или папка отправляется в небытие... И даже мощные программы восстановления могут помочь далеко не всегда – даже если с момента удаления файла прошло всего несколько минут!

Ирония судьбы – пока одни выжимают из себя последние капли пота, пытаясь информацию восстановить, другие спят и видят, как бы ее УДА-

ЛИТЬ. Начисто. И чтобы «оживить» ее было невозможно даже теоретически. Бизнесмены, политики... Да мало ли кому может понадобиться эдакий «измельчитель» для файлов?

Казалось бы – в чем проблема? Отправил файл в Корзину, очистил ее для пущей надежности – и спи спокойно!

Не торопитесь – все не так уж просто...

Как вы знаете, каждый файл на нашем компьютере, как правило, разбросан по различным участкам диска в виде фрагментов. А вся информация о том, какие секторы диска соответствуют этому файлу, хранится в специальной базе данных – File Allocation Table (FAT). Так вот – удаляя файл или папку, мы просто стираем из FAT все сведения о них – занятое информационными «кусочками» пространство считается теперь свободным!

Но на самом деле таковым оно не является – сама информация никуда с диска не делась! Она по-прежнему «дремлет» в занятых ячейках... А значит, чтобы восстановить такой «удаленный» файл, достаточно отыскать предыдущую копию FAT, вернув удаленную запись на место.

Не помогает и полное форматирование диска – по тем же причинам. И даже если с момента «смерти» файла прошло много времени,

и в его бывшие сектора уже вселилась другая информация, шанс вернуть утраченное есть – правда, уже не дома, а в специальных лабораториях.

И лишь специальные утилиты для «безвозвратного» удаления могут покончить со строптивыми файлами раз и навсегда – они не просто изменяют FAT, но и добросовестно вычищают все необходимые сектора жесткого диска, «забивая» каждый из них нулями и единицами до 10 раз кряду! Вот почему такими программами охотно пользуются в крупных корпорациях, научных и правительственных учреждениях...

А кое-кто считает, что и дома без них не обойтись!

Acronis Drive Cleanser

(http://www.acronis.ru)

Надежное средство уничтожения данных на жестких дисках.

Acronis Drive Cleanser 6.0 гарантированно уничтожает данные на выбранных разделах или/и дисках.

Избавляетесь от старого компьютера, устанавливаете новый жесткий диск, возвращаете арен-

дованный компьютер, или переустанавливаете все на компьютере вашей компании? Тогда просто необходимо надежно избавиться и гарантированно уничтожить все данные на старом или возвращаемом жестком диске.

Пресса и Интернет полны сообщениями о случайно приобретенных компьютерах (при распродаже имущества ликвидируемых компаний), на жестких дисках которых осталась конфиденциальная информация: персональные данные сотрудников (номера лицевых счетов в банке, кредитных карточек, карт социального обеспечения, размер заработной платы), бухгалтерские и другие внутренние документы, материалы совещаний советов директоров.

Конфиденциальная информация должна не только храниться с соблюдением строгих правил, но и надежно уничтожаться! Удаление файлов данных средствами операционной системы, форматирование разделов жестких дисков и их удаление не гарантируют невозможности восстановления информации специальными программными или аппаратными средствами. Гарантированное уничтожение конфиденциальной информации возможно только с помощью специально разработанных программ, реализующих зачастую довольно сложные алгоритмы.

Основные возможности и особенности программы:

- Гарантированное удаление всех данных и разделов на жестком диске.
- Возможность – наряду с очисткой – отформатировать диск или раздел диска, или удалить раздел.
- Возможность увидеть результаты выполнения сценария уничтожения информации раздела или/и жесткого диска с помощью встроенной программы DiskViewer.
- Очень удобный в использовании интерфейс в стиле Windows XP в виде Мастера подсказок.

Стандарты уничтожения данных:

- Американский: DoD 5220.22-M
- Американский: NAVSO P-5239-26 (RLL)
- Американский: NAVSO P-5239-26 (MFM)
- Германский: VSITR
- Российский: GOST P50739-95

Два значительно более мощных предопределенных алгоритма, предложенных наиболее авторитетными экспертами по информационной безопасности:

- Алгоритм Питера Гутмана
- Алгоритм Брюса Шнайера

Paragon Disk Wiper

(http://www.paragon.ru)

Не оставляйте свою конфиденциальную информацию на старом жестком диске. После удаления данных обычным путем их можно восстановить.

Paragon Disk Wiper поможет безвозвратно удалить любые данные с жесткого диска. Позволяет затирать как целые диски и разделы, так и только свободное место на разделе, временные папки, файлы, а также временные файлы, cookies, history для браузеров и ICQ.

Пароли

Парольная защита информации является наиболее распространенной. Вы с ней сталкиваетесь везде: и входя в сеть, и проверяя почту, и заглядывая на «закрытый» сайт... Но есть у паролей и одно неприятное свойство: их надо запоминать. А человек, наоборот, любит что-нибудь забывать, причем, как правило, в самый неподходящий момент. Поэтому пароли часто записывают на бумажку или используют один и тот же «любимый» пароль всюду, что в значительной степени повышает риск того, что он будет «взломан».

Осмелимся дать несколько советов, которые, возможно, смогут облегчить жизнь не только вам, но и системному администратору:

- Постарайтесь избегать таких «сложных» паролей как ваше имя, имя вашей собаки, день рождения и т. п.
- Не стоит в качестве пароля использовать осмысленные слова – при подборе пароля по словарю такой пароль «ломается» очень быстро.
- Если уж вы записываете пароль на бумажку (чего мы делать не рекомендуем), то хотя бы запишите его в обратном порядке или добавьте какие-нибудь символы в определенных позициях.
- Желательно использовать разные пароли для разных сервисов, при этом даже если злоумышленник узнает какой-то из ваших паролей, то не все будет потеряно...
- Не используйте пароли короче 6–8 символов.

Разумеется, все эти рекомендации могут остаться пустыми пожеланиями – мало кто способен придумать и запомнить пару десятков случайных паролей, но, к счастью, есть и способы облегчить эту задачу. Во-первых, существуют специальные программы, которые позволяют хранить множество паролей в единой зашифрованной базе данных – таким образом вам надо

будет запомнить только один пароль от этой базы. Во-вторых, существуют и программы для генерации случайных паролей, причем нередко эти две функции объединяются в одной программе. Ну а если все-таки придется выдумывать пароль самостоятельно, то выберите какое-нибудь запоминающееся предложение и образуйте пароль из него, скажем, «киоск по продаже спиртных напитков» и пароль «кипопроспина». И запомнить достаточно несложно и подбирать долго... А вместо того, чтобы записывать в записную книжку готовый пароль, запишите что-нибудь, что по ассоциации заставит вас вспомнить ключевую фразу. Поверьте, это работает!..

Ну и, наконец, еще один совет, который, правда, больше относится к разделу «шифрование» – не доверяйте ваши важные документы программам, которые не специализируются на сохранении данных. Очень часто документы в офисах «закрывают» встроенными средствами MS Word – этого делать не стоит. Чуть более надежно, но все равно недостаточно для конфиденциальной информации – архивирование с паролем. Лучше воспользуйтесь чем-нибудь вроде бесплатного scramdisk-a...

PasswordSafe

(http://passwordsafe.sourceforge.net/)

Эта программа позволит вам хранить все ваши пароли в одном месте (не в том, о котором

вы подумали, а в файле). Пароли могут группироваться по темам и снабжаться комментариями. Сам файл, в котором все пароли записаны, тоже шифруется с паролем, но ведь запомнить один пароль намного проще, чем пару десятков? В программу встроена и утилита для генерирования паролей.

SecureWord

(http://www.cezeo.ru)

Программа SecureWord изначально разрабатывалась как наиболее удобная и в то же время полнофункциональная программа для хранения важной информации (паролей, логинов и т. д.).

Поскольку подобные программы уже существуют, позвольте вам объяснить, чем наша программа отличается от всех остальных.

⏭ Действительно надежные и современные алгоритмы защиты информации (шифрования). Основной алгоритм который используется в SecureWord, это – AES, Advanced Encryption Standard. И это именно стандарт, принятый Американским правительством в 2002 году для повсеместного использования. Мы используем наиболее надежную конфигурацию, с самым большим ключом.

⏭ Улучшенная система безопастности. Не секрет, что пока данные находятся в памяти компьютера, они наиболее уязвимы. У нас используются две функции, которые наиболее полно устраняют этот эффект: а) очистка буфера обмена при выходе из программы; б) выгрузка данных пользователя при минимизации, например, вы можете быстро найти нужный пароль, использовать его и нажать кнопку **Минимизировать**.

⏭ Удобный и опрятный интерфейс, мы всегда уделяем ему большое внимание – поскольку от качества интерфейса зависит удобство вашей работы.

⏭ Быстрый и настраиваемый поиск, достаточно ввести в строке поиска нужное слово (или часть его), как тут же вы увидите список заметок, содержащих его. Можете дописывать слово или, наоборот, стирать буквы из строки – список будет обновляться динамически!

⏭ Ничем не ограниченная база заметок. Храните столько, сколько хотите. Заметки, папки и файлы!

⏭ На одном компьютере может быть сколько угодно пользователей – у каждого будет своя база заметок.

⏭ В программу включен Генератор стойких (надежных) паролей – поскольку теперь о ваших паролях будет заботиться SecureWord и можно не бояться их забыть. Теперь можно задавать действительно сложные пароли для доступа и наш генератор отлично справляется с этой задачей.

⏭ Для того чтобы перенести базу заметок на другой компьютер (например, на ноутбук), достаточно скопировать всего один файл! SecureWord сама подскажет, какой файл. Так же поддерживается интеграция с BackUp программой BackUpTime.

⏭ Всесторонняя справка – на каждое окно программы, на каждое действие. И естественно, список советов и рекомендаций.

⏭ Цена, да, цена! SecureWord стоит всего 200 рублей, не $20 и не $15, а всего 200 рублей. Согласитесь, что она этого стоит.

Контроль изменений в системном реестре

WinPatrol

(http://www.winpatrol.com)

Одна из самых удобных программ для пользователей со стажем. Эта бесплатная утилита позволяет контролировать установку разнообразных нежелательных программ — Spyware, Adware и т. п. (в базу данных включено описание примерно 14 000 вредоносных программ). Для этого контролируются важные системные области (область загрузки, системные папки, реестр), которые обычно изменяются подобными нежелательными программами. Программа работает как в режиме сканера, так и постоянного монитора.

WinPatrol – это не столько простая «чистилка», вроде Spyware Doctor, сколько расширенный «менеджер процессов». Монитор позволяет отследить все программы, сервисы и процессы, активные в данный момент на вашем компьютере – их описания грамотно сгруппированы по специализированным вкладкам: автозагрузка, дополнительные модули Internet Explorer, сис-

темные сервисы, активные задачи и так далее. Стандартная версия программы практически не позволяет вносить изменения в конфигурацию системы, расширенный же вариант предоставит вам подробную информацию по каждому процессу.

RegRun Security Suite

(http://www.greatis.com)

Одна из самых популярных программ для защиты системного реестра от незаконных вторжений со стороны вирусов и «троянских» программ. Заодно эта утилита позволяет вам отследить, какие именно изменения в реестр вносят во время установки и работы обычные программы.

Для новичков возможности программы могут показаться излишними (так оно и есть), к тому же достаточно высокая стоимость программы выводит ее из разряда «домашних». А вот для профессионалов – это, что называется, самое оно.

Краткая аннотация:

Резидентный монитор (Watch Dog) и утилита защиты системных файлов (System Files Protection) отслеживают внесение изменений в

списки автозапуска, реестр и системные файлы в течение всего сеанса работы Windows, а при обнаружении изменений позволяют произвести откат.

Кроме этого программа умеет реализовывать пакетный и отложенный запуск необходимых программ, взаимодействовать с наиболее популярными антивирусными пакетами и предупреждать пользователя о необходимости проверки тех или иных файлов на предмет их заражения вирусами, выводит список всех открытых на данный момент файлов, имеет утилиту Registry Assistant для работы с реестром и функцию Black List для автоматической блокировки запуска новых приложений. Имеется также база данных приложений (Application Database), используя которую, утилита Watch Dog следит за запуском приложений и при возникновении вопросов извещает об этом пользователя.

Выпущена в трех модификациях, различающихся своей функциональностью:

- RegRun Standart
- RegRun Pro
- RegRun Gold

В самую мощную версию Gold дополнительно включены утилиты WinCleaner (для очистки

диска и кэша), Trojan Analyser (анализатор поведения программ для обнаружения «троянов») и Rescue (резервное копирование реестра и системных файлов), а в разработке находятся модули мониторинга портов и проверки скриптов и макросов.

RegProtection

(http://www.stonebrowser.narod.ru)

Эта небольшая утилита, конечно, не может по-настоящему конкурировать с предыдущей программой. Зато она компактна, бесплатна, да и общается с вами по-русски. Словом – отличная программа из разряда «на всякий случай», достаточно функциональная и удобная.

Программа, ведущая контроль нескольких «опасных» точек реестра, а именно: секций RUN и RUNONCE, в которые обычно прописываются разные «трояны», бэкдоры, вирусы (независимо от того, известны или неизвестны они антивирусу) и прочие гадости, дабы навеки завладеть вашим компьютером.

После запуска программа остается в памяти компьютера. Если в контролируемом разделе происходит изменение (добавление/удаление записи), то программа немедленно вас предупредит и предложит удалить вновь добавленное.

Возьмем, к примеру вирус BLAST (LOVSAN). Самостоятельно запускается файл MSBLAST.EXE. При этом в разделе

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

появляется запись:

windows auto update=msblast.exe,

которая, собственно, и приводит к загрузке вредоносной программы в память.

RegProtection имеет возможность удалить эту запись сразу же после ее обнаружения, лишив вирус возможности запуститься без вашего ведома в следующий раз.

ИНТЕРЕСНЫЕ ПРИМОЧКИ

Программы для заполнения форм и хранения паролей

Работая с сайтами Интернета, мы постоянно сталкиваемся со всевозможными формами и бланками, которые необходимо трудолюбиво заполнять. Оформление покупки в «виртуальном магазине», подписка на новости сайта или почтовую рассылку, регистрация вашей странички в базе данных поискового сервера — все эти действия потребуют от вас ввода определенных данных о собственной персоне. Делать это, поверьте, приходится достаточно часто. И простая на первый взгляд процедура превращается в утомительную рутину. Тем более что вводить-то приходится каждый раз одни и те же, стандартные данные: электронный и почтовый адрес, имя-фамилию-отчество, год рождения и прочее.

Другой бич пользователей со стажем — обилие паролей и «логинов», необходимых для доступа ко многим сайтам. Например, к вашей собственной страничке статистики на сервере провайдера. А в дальнейшем количество «бдительных» страниц и сайтов в вашем «путевом дневнике» возрастет многократно — а стало быть, вам придется держать в голове множество логинов и паролей.

Понятно, что голова — не самый лучший банк для столь важных сведений. Куда надежнее записывать эти пароли в записную книжку, но как в этом случае быть с безопасностью? Книжку вы можете потерять, к ней могут получить доступ самые разные люди... Что отнюдь не желательно — особенно если учесть, что в ряде случаев пароль для доступа на сайт может позволить постороннему запустить любопытный глаз, а то и загребущую ручонку, в ваш банковский счет...

Даже если я намеренно сгустил краски, реальная картина именно такова: хранить пароли в голове — ненадежно, на бумаге — небезопасно. И в обоих случаях — просто неудобно.

По столь длинному вступлению вы уже догадались, что речь в этой главе пойдет о программах, способных решать обе эти проблемы сразу: сохранять данные, введенные вами в типовые

«бланки» различных сайтов, и в дальнейшем заполнять нужные строчки автоматически, пользуясь собственной базой данных. А заодно, при необходимости, запоминать пароли и логины к разнообразным сайтам — причем сохранять их таким образом, чтобы эта «виртуальная копилка» допускала к себе лишь своего главного пользователя. То есть вас...

AI RoboForm

(http://www.roboform.com)

Просто удивительно, как мало пользователей Сети осведомлено о существовании этой небольшой, но весьма функциональной программы. К тому же — созданной отечественными программистами, а значит, способной общаться с пользователем на родном языке без какой-либо дополнительной настройки или внешних модулей.

Программа включает в себя два главных компонента:

- Identities — Книга персон. В ней хранятся данные для каждого пользователя Roboform (их ведь может быть несколько!). Создавая «пер-

сону», вы должны заполнить подробную анкету с типовыми вопросами (адрес, возраст и так далее). Позднее эти значения будут подставляться при заполнении типовых форм. В профессиональной версии вы сможете не только использовать уже имеющиеся поля типовой анкеты, но и создавать новые.

⏭ PassCards — Книга паролей. Подобно тому, как «книга персон» сохраняет ваши персональные данные, «книга паролей» будет сохранять логин и пароль для доступа к сайтам. Причем для этого вам уже не нужно вводить их в базу данных: программа сама сохранит все необходимое в тот момент, когда вы наберете логин и пароль в первый раз. Просмотреть и изменить базу данных программы вы сможете с помощью пункта Просмотр книги паролей контекстного меню Internet Explorer.

Для каждого сайта в базе данных программы создается отдельная запись: в режиме просмотра книги паролей вы можете изменить или удалить ее, а также защитить запись паролем — таким же образом, как и в «книге персон». Правда, теперь вас вновь будет тревожить «всплывающее окошко», требующее ввести главный пароль... Но что для вас важнее — удобство или безопасность — вы, надеюсь, решите и без моей подсказки...

Помощник заполнения форм

(http://www.keepsoft.ru/qis.htm)

Компактная заполнялка форм на веб-страницах от автора «Домашней Бухгалтерии» Павла Козловского.

Информация разработчика: ...Помните, сколько раз приходилось заполнять веб-формы, которые содержат одни и те же вопросы? Эта программа сильно облегчит вам жизнь: вы введете ответы на общие вопросы один раз, а затем, когда понадобится заполнить какую-нибудь анкету, просто щелкните по значку в трее и выберите нужный ответ, который будет помещен с clipboard. Программа просто необходима любому веб-серферу.

Password Commander

(http://www.pascom.ru)

На гениальном, но платном RoboForm свет клином не сошелся: существует множество других менеджеров для хранения паролей и автоматического заполнения форм на страницах Интернета. Один из них, Password Commander, российские пользователи могут получить абсолютно бесплатно (зато пользователям из других стран программа обойдется в 50 долларов). Правда, разработчики

все-таки просят поддержать их труд полновесным рублем — и это настоятельно рекомендуется сделать, поскольку программа и впрямь вышла удачная.

Возможности программы:

- Хранит пароли и личные данные в одной базе.
- Автоматически заполняет формы на сайтах и вводит данные в окна программ, нажимает кнопку «Войти» за вас, ведь время — самый ценный ресурс. Автозаполнение поддерживается во всех распространенных браузерах: Internet Explorer, Opera, Maxthon, Mozilla, Firefox.
- Генерирует надежные пароли — пароль «Сидоров» подбирается в течение нескольких часов, обезопасьте себя от этого.
- Поддерживает более 40 плагинов шифрования — никто не получит доступ к вашим данным.
- Совместим с биометрическими устройствами — Password Commander узнает вас по отпечатку пальца.
- Распознает пользователей автоматически, когда пользователь входит в свой Windows-аккаунт — зачем набирать пароль дважды?
- Создает личный аккаунт для каждого члена вашей семьи — будьте спокойны за свои пароли.

- Работает с переносных носителей (USB-флеш) — держите пароли под рукой.
- Делает резервную копию, экспортирует/импортирует и печатает пароли — все для удобства.
- Защищает от программ key-логеров, предоставляя возможность вводить пароли через экранную клавиатуру.
- Работает с файлами.

СОХРАНЯЕМ И ВОССТАНАВЛИВАЕМ

Уже неоднократно было сказано, насколько могут быть коварны современные вирусы, и что стопроцентную защиту обеспечить не может ни одна программа.

Если «вредители» все-таки нашли брешь в системе вашего компьютера, и вы пострадали, готовьтесь к тому, что после лечения зараженной персоналки могут возникнуть другие проблемы. Например, не откроется флешка или локальный диск, «побьются» файлы или программы начнут вести себя странно. К сожалению, антивирусы не смогут восстановить нарушенные системные настройки, а радикальный метод – переустановка операционки – не всегда приемлем. Поэтому остается только восстановление вручную. В помощь нам – набор программ.

Сохранение и восстановление конфигурации

Нужно ли и можно ли заменять стандартные программы восстановления системы какими-то сторонними утилитами?

Нужно — ибо при всех своих достоинствах характер у этой ремонтных дел дамы весьма капризный. Скажем, подключили вы к системе внешний жесткий диск, создали точку восстановления... Думаете, что после того, как вы отключили ваш флеш-брелок или мобильный винчестер, вы не испытаете никаких трудностей с «откатом»? Ах, надежда, компас ты наш земной...

Словом, ежели вы заядлый рискач и ваша система постоянно находится под угрозой «слета», придется нам искать что-то получше. Хотя искать не надо — вот вам, пожалуйте, несколько программ на выбор:

Driver Genius

(http://www.driver-soft.com)

АБСОЛЮТНО незаменимая программа для тех, кому часто приходится переустанавливать

Windows. Скорее — даже ОБЯЗАТЕЛЬНАЯ (наряду с WinRescue и Ashampoo Uninstaller). Именно так — большими буквами. Driver Genius позволяет вытащить из уже установленной копии Windows все драйверы и сохранить их на диске — как в собственном архивном формате программы, так и в виде исполняемого файла. А это значит, что после переустановки системы вам не надо будет возиться с многочисленными дискетами и CD — все драйверы будут установлены одним щелчком мышки. Только не пытайтесь таким образом перетаскивать драйверы с ДРУГОГО компьютера — нарветесь на крупные неприятности.

Мало того — Driver Genius позволяет в автоматическом режиме найти обновленные драйверы для всех установленных в систему устройствах. Поддерживается работа с более чем 30 тысячами различных материнских плат, видеокарт, звуковых и сетевых карт, модемов, мониторов, клавиатур, мышей, видеокамер и т. д. База программы постоянно обновляется.

Имеется поддержка русского языка.

ShadowUser

(http://www.shadowstor.com/)

Отчаянные рискачи, любители устанавливать на компьютер «левый» софт и экспериментировать со своей системой до полного посинения

экрана с криками восторга вознесут эту программу на щит. Еще бы — благодаря ей вы сможете творить со своим компьютером все, что душе угодно: устанавливать программы любой степени сомнительности, превращать жесткий диск в рассадник вирусов и даже удалять важные системные файлы. Интернетчики оценят возможность бродить по сомнительным сайтам без риска заполучить на свой компьютер кучу заразы — причем без всякого файрволла или антивируса. В том случае, если вы активировали «теневой» режим работы этой программы, все эти фокусы не приведут к фатальным последствиям: после перезагрузки компьютера все вернется в норму. Достигается это за счет довольно изящного трюка: программа не создает резервных копий реестра и файловой системы, а формирует новый, «виртуальный» компьютер, используя для хранения информации незанятые секторы жесткого диска. Таким образом, при защите жестких дисков или важных папок никакие изменения в них не будут записаны в реальное «оглавление» диска — таблицу размещения файлов. Изменения коснутся лишь «виртуальной» файловой системы ShadowUser, которая бесследно исчезнет после перезагрузки. Впрочем, если вы захотите по завершении сеанса работы принять все сделанные изменения, программа позволит вам это сделать. Кстати, некоторые папки (например, для документов или скачанных из сети файлов) можно оставить незащищенными, внеся их в список исключений.

GoBack

(http://www.symantec.com)

Большинство утилит «отката», позволяющих вернуться к стабильному состоянию системы в случае сбоя, ограничиваются лишь созданием резервных копий реестра и, в редких случаях, созданием дополнительных конфигурационных файлов. Но в случае фатальных сбоев, связанных, например, с повреждением файловой системы, такие утилиты оказываются бессильны. Вот на такой случай и подойдет программа GoBack, самый распространенный и доступный зверь из породы «восстановителей» конфигурации. Проживает он в знаменитом пакете утилит Norton System Works, где, похоже, чувствует себя совсем неплохо.

Но зато — и функциональность зверушки на высоте. GoBack добросовестно отслеживает и фиксирует все изменения, внесенные в информационную структуру компьютера, любую модификацию файловой системы. Программа денно и нощно сторожит ваш компьютер, оставаясь невидимой и неслышимой. Впрочем, это все-таки громко сказано: GoBack пусть не слишком заметно, но все же «притормаживает» ваш компьютер. К тому же для хранения собственных «протоколов» программа взимает с вашего винчестера «десятину» (действительно, под «склад» GoBack резервируется около 10 % емкости диска, а в «сетевой» версии — даже до 20).

Действительно, зверь — мощный, огромный, неторопливый. А посему применение GoBack могут себе позволить только пользователи с избытком оперативной памяти, да и процессором не из последних.

Но в случае сбоя преимущества такого подхода станут видны сразу. Во-первых, благодаря дотошности GoBack вы сможете «вернуться в прошлое», откатившись не только на день, но и на час, и даже на несколько минут назад! Если при установке какой-то программы или драйвера были испорчены или заменены важные системные файлы, GoBack восстановит и их.

Интересно, что, восстанавливая содержимое диска, можно не просто «наложить» старую копию файловой системы на новую. GoBack предусматривает и иной вариант — создание нового раздела, на котором будет смонтирована точная копия вашего диска на момент сохранения последней «точки отката». Конечно, такой вариант возможен только при наличии второго жесткого диска, либо достаточного свободного пространства на первом.

Кстати, с помощью программы можно восстановить не только диск целиком, но и отдельные файлы и папки — это может помочь при потере или порче важного документа.

Еще одно преимущество GoBack заключается в возможности запустить процесс восстановле-

ния еще до загрузки Windows: меню восстановления можно вызвать сразу после включения компьютера.

NikSaver

(http://www.niksaver.com)

Информация разработчика:

Программа создана для хранения настроек. Как бывает обидно терять месяцами, а то и годами созданную рабочую среду компьютера, настройки программ и игр, закладки, фильтры и т. д. Теперь можете забыть об этом. Программа NikSaver позволяет сохранить все настройки для системы, программ и игр и при необходимости также легко восстановить их. При запуске программа автоматически определяет установленные у вас программы и выводит в список. Сохранение и загрузка настроек проходят тоже в автоматическом режиме — достаточно выбрать нужную программу или программы и кликнуть по кнопке «Сохранить» или «Загрузить». Сейчас NikSaver поддерживает более 200 программ и игр. Также есть возможность добавления своих программ и игр.

Restore-It

(http://www.farstone.com)

Программа от Farstone, по сути, берет на себя ту работу, которую доселе выполняла стандарт-

ная программа System Restore, причем после ее установки штатного «защитника» Windows можно просто удалить — чтобы не путался под ногами. Поскольку SecurePC к работе подходит куда ответственнее. Ведь она не просто копирует реестр, важные системные файлы и документы в специальную папку, но и создает под хранилище новый, скрытый от глаз пользователя раздел на жестком диске (около 10 % его объема).

Что это дает? Ну, во-первых, предохраняет резервные копии от слишком внимательных глаз и шаловливых ручек пользователей. А во-вторых (внимание!) дает возможность запустить процесс восстановления еще ДО загрузки Windows! Так что вам не придется в случае серьезного сбоя связываться со всяческими Safe Mode — достаточно нажать пробел в начале загрузки компьютера и выбрать нужную вам точку восстановления. Вуаля!

Кстати — создавать точки восстановления, равно как и восстанавливать систему, компьютер может в полностью автоматическом режиме согласно заданному вами расписанию.

Windows Backup Wizard

(http://www.risingresearch.com/ru/)

Чем больше вы устанавливаете новых программ, тем медленнее и неустойчивее начинает работать вся система. Для того, чтобы не при-

шлось переустанавливать Windows, необходимо всегда иметь ее резервную копию. Программа Windows Backup Wizard позволит вам легко создать и восстановить резервную копию Windows, и при этом сэкономит вам место на диске!

Программа позволяет создать копию всей операционной системы Windows или только отдельных файлов и папок.

Вы можете не проводить резервное копирование файлов, если они есть в предыдущих копиях, тогда размер новой копии уменьшится на 85-95 процентов и вам понадобится значительно меньше времени, чем при создании обычной копии.

Отказ от резервного копирования файлов, которые есть в дистрибутиве Windows, — еще один способ создать резервную копию меньшего размера. В этом случае размер копии только что установленной Windows будет занимать всего несколько мегабайт.

Windows Backup Wizard позволяет использовать «Планировщик заданий» для проведения операции резервного копирования через определенные промежутки времени.

Использование профилей резервного копирования значительно облегчит вам процесс создания копий, так как один раз задав необходимые установки, в дальнейшем вам не нужно будет

вновь настраивать необходимые параметры перед началом резервного копирования.

Windows Backup Wizard позволяет проводить ускоренное восстановление копии Windows, что достигается за счет отказа от восстановления неизменившихся файлов.

С Windows Backup Wizard вы можете использовать любой архиватор, главное, чтобы он имел поддержку длинных имен и умел работать со списком файлов (практически все современные архиваторы удовлетворяют этим требованиям).

Windows Backup Wizard позволяет просмотреть информацию обо всех созданных резервных копиях (занимаемое место на диске, требуемое место при распаковке и т. д.) и удалить ненужные копии.

Windows Backup Wizard имеет простой и удобный интерфейс, позволяющий последовательно пройти все необходимые этапы создания или восстановления копии Windows.

Содержание

Предисловие 3

Уголок Остапа Бендера: сетевые аферы 5
«Нигерийские письма» 10
«Фишинг» 12
«Порно-сайт» и «магазин конфиската» 15
«Free GSM» 16
«Генераторы карт» 21
Виртуальный «обменник» 24
«Заработок в Интернете» 26
«Музыкальная кладовая» 31

Защита от вредоносных программ 35
Вирусы 37
Классические вирусы-«паразиты» 45
Вирусы-программы (W32) 48
Макровирусы 51
Скрипт-вирусы 55
«Троянские» программы и руткиты 62
«Шпионские» программы и рекламные модули . . 71
Лучшие средства защиты 76
Антивирусные программы 79
Программы для удаления Spyware и Adware . . . 86
Ad-aware 88
Spyware Doctor 91
Межсетевые экраны (файрволлы) 93
Центр безопасности Windows 102

Outpost Firewall 104
ZoneAlarm 110

Конфиденциальность и приватность в WWW 113
Прокси-серверы 114
Веб-маскировщики и «анонимайзеры» 122
Как «замести следы» при работе в Сети 124

Аптечка: на все случаи жизни 133
Безопасность в Интернете 133
Многофункциональные пакеты 135
Kaspersky Personal Security Suite 135
Norton Internet Security 137
McAfee Internet Security Suite 141
Антивирусные программы 144
Dr.Web 149
Norton Antivirus 151
Panda Antivirus 154
Avast 156
AVG Antivirus 157
Remove It! 158
Clrav 159
Защита от «троянских» программ 160
PestPatrol 163
Trojan Remover 163
Защита от Spyware и Adware 164
AVG Anti-Spyware 168
Программы для защиты от «взломов» (файрволлы) 169
PortsLock 173
Ashampoo Firewall 173
Comodo Firewall 174
Анонимный серфинг и приватность 176
Hide IP Platinum 178
Hider IP 179
Don't Panic! privacy software 180
IE Security Pilot 180
ProxyChecker 181
SocksChain 183
Shadow Professional 184

Средства шифрования ... 185
PGP Desktop ... 185
SecureFX ... 186
Информационные утилиты ... 187
SmartWhois ... 187
Ping Plotter ... 188
WinDump ... 188
VisualRoute ... 189
Whois, Finger, and Host Utilities ... 190
Мониторы ... 191
HostMonitor ... 191
Сканеры ... 192
ShadowSecurityScaner ... 192
PC Security Test ... 193
PC Super Scanner ... 194
CommView ... 194
Программы для борьбы со спамом ... 195
Kaspersky Anti-Spam ... 201
MailWasher ... 202
SpamPal ... 204
Средства шифрования и управления доступом 206
Ashampoo Magical Securiy ... 206
DriveCrypt ... 207
Steganos Security Suite ... 208
Private disk ... 209
Hide Folders XP ... 211
DeviceLock ... 213
Folder Lock ... 214
TrueCrypt ... 215
Folder Guard ... 216
LockWin ... 217
Mouse Trap ... 218
Безвозвратное удаление информации ... 219
Acronis Drive Cleanser ... 221
Paragon Disk Wiper ... 224
Пароли ... 224
PasswordSafe ... 226
SecureWord ... 227

Контроль изменений в системном реестре 230
WinPatrol 230
RegRun Security Suite 231
RegProtection 233
Интересные примочки 235
Программы для заполнения форм и хранения паролей 235
AI RoboForm 237
Помощник заполнения форм 239
Password Commander 239
Сохраняем и восстанавливаем 242
Сохранение и восстановление конфигурации 243
Driver Genius 243
ShadowUser 244
Go Back 246
NikSaver 248
Restore-It 248
Windows Backup Wizard 249

Справочное издание

Леонтьев Виталий Петрович

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

Зав. редакцией *Г. Г. Утенов*
Редактор *С. Ю. Устюжанина*
Художественный редактор *И. Н. Васильев*
Компьютерная верстка *О. П. Солововой*
Корректор *О. Ю. Ашмарина*

Подписано в печать 15.01.2008.
Формат 84×108$^{1}/_{32}$. Гарнитура «Ньютон».
Бумага газетная. Печать офсетная.
Усл. печ. л. 13,44. Тираж 2000 экз.
Изд. № 07-8912. Заказ № 2135.

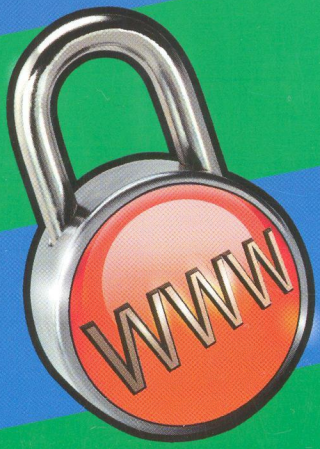
ЗАО «ОЛМА Медиа Групп»
105062, Москва, ул. Макаренко, д. 3, стр. 1
http://www.olmamedia.ru

Отпечатано в ОАО «ЧПК»
Сайт: www.chpk.ru E-mail: marketing@chpk.ru
Факс 8(49672)6-25-36, факс 8(496) 270-73-59
Отдел продаж услуг многоканальный: 8(499) 270-73-59

Компьютер это просто

ВМЕСТЕ С ИНТЕРНЕТОМ
В НАШУ ЖИЗНЬ ВОШЛИ
ТАКИЕ ЯВЛЕНИЯ,
КАК КОМПЬЮТЕРНЫЕ ВИРУСЫ,
«ТРОЯНЫ», СПАМ И ДРУГИЕ
НЕ СЛИШКОМ ПРИЯТНЫЕ ВЕЩИ.
НОВАЯ КНИГА ВИТАЛИЯ ЛЕОНТЬЕВА
ПОМОЖЕТ КАК ОПЫТНОМУ,
ТАК И НАЧИНАЮЩЕМУ
ПОЛЬЗОВАТЕЛЮ
МАКСИМАЛЬНО ОБЕЗОПАСИТЬ
СВОЙ КОМПЬЮТЕР
ОТ АТАК ИЗ СЕТИ.
КРОМЕ ТОГО, ВЫ УЗНАЕТЕ:

КАК РАСПОЗНАТЬ СЕТЕВОЕ МОШЕННИЧЕСТВО
ОТКУДА ПОЯВИЛИСЬ ВИРУСЫ И КАКИЕ ОНИ БЫВАЮТ
КАК ЗАЩИТИТЬСЯ ОТ ВРЕДОНОСНЫХ ПРОГРАММ
КАК ОБЕСПЕЧИТЬ СЕБЕ КОНФИДЕНЦИАЛЬНОСТЬ В СЕТИ
КАК СОХРАНИТЬ СВОИ ПАРОЛИ В БЕЗОПАСНОСТИ



ISBN 978-5-373-01819-7
ОЛМА МЕДИА ГРУПП
9 785373 018197